Security Assessment Report for itsecgames.com

1. Executive Summary

This report presents a thorough security assessment of `itsecgames.com`, focusing on detection of vulnerabilities, security misconfigurations, SSL/TLS health, and information exposure risks. The goal is to identify actionable security weaknesses and provide prioritized mitigation recommendations to improve resilience against potential cyberattacks.

2. Scope and Objectives

- **Target:** http://www.itsecgames.com/ (IP: 31.3.96.40)
- **Objectives:**
  - Identify web and network vulnerabilities via automated tools.
  - Detect outdated software components and CVEs.
  - Assess SSL/TLS certificate validity and protocol strength.
  - Highlight exposed headers, error messages or banners.
  - Present prioritized findings and remedial actions

3. Methodology

The assessment followed three key phases:

1. **Reconnaissance & Information Gathering:** WHOIS queries, DNS enumeration, and technology fingerprinting with `whatweb`.
2. Automated Vulnerability Scanning: Using `Nikto` for web server analysis and `Nmap` for port & vulnerability enumeration.
3. **SSL/TLS Evaluation:** Certificate and protocol analysis using OpenSSL and Qualys SSL Labs.

All results were documented with included command outputs and screenshots.

4. Detailed Findings

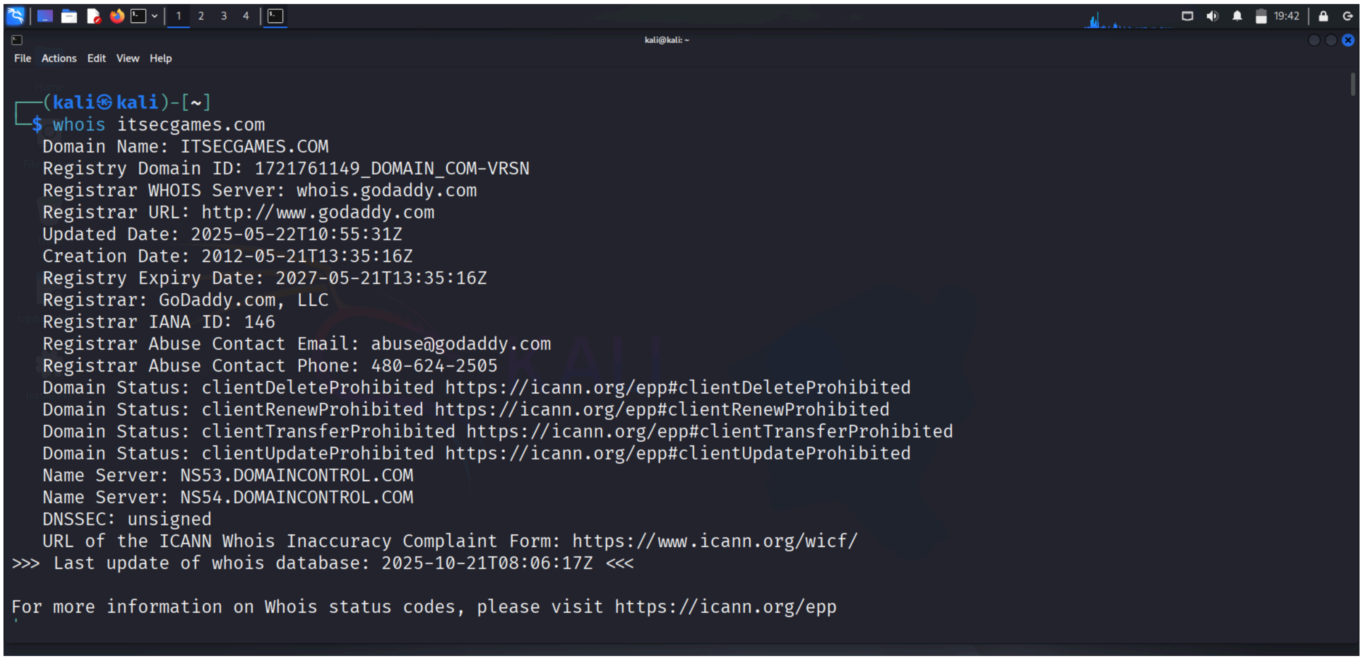
4.1 Reconnaissance & Information Gathering

WHOIS Lookup:

```
WHOIS Lookup:
┌──(kali㉿kali)-[~]
```

```
└─$ whois itsecgames.com
   Domain Name: ITSECGAMES.COM
   Registry Domain ID: 1721761149_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2025-05-22T10:55:31Z
   Creation Date: 2012-05-21T13:35:16Z
   Registry Expiry Date: 2027-05-21T13:35:16Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited
https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited
https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited
   Name Server: NS53.DOMAINCONTROL.COM
   Name Server: NS54.DOMAINCONTROL.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form:
https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-21T08:06:17Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
```

```
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
This WHOIS server is being retired. Please use our RDAP service instead. Rate
limit exceeded. Try again after: 2562047h47m16.854775807s.
```



```
┌──(kali㉿kali)-[~]
└─$ whois itsecgames.com
   Domain Name: ITSECGAMES.COM
   Registry Domain ID: 1721761149_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2025-05-22T10:55:31Z
   Creation Date: 2012-05-21T13:35:16Z
   Registry Expiry Date: 2027-05-21T13:35:16Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS53.DOMAINCONTROL.COM
   Name Server: NS54.DOMAINCONTROL.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-21T08:06:17Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

- Domain registered via GoDaddy since 2012; expires 2027.
- Name servers: ns53.domaincontrol.com, ns54.domaincontrol.com.
- DNSSEC not implemented.

DNS Queries:

```
─(kali㉿kali)-[~]
└─$ dig itsecgames.com
```

```
; <<>> DiG 9.20.9-1-Debian <<>> itsecgames.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;itsecgames.com.                        IN      A

;; ANSWER SECTION:
itsecgames.com.         600     IN      A       31.3.96.40

;; Query time: 1848 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Tue Oct 21 13:38:50 IST 2025
;; MSG SIZE  rcvd: 59
```

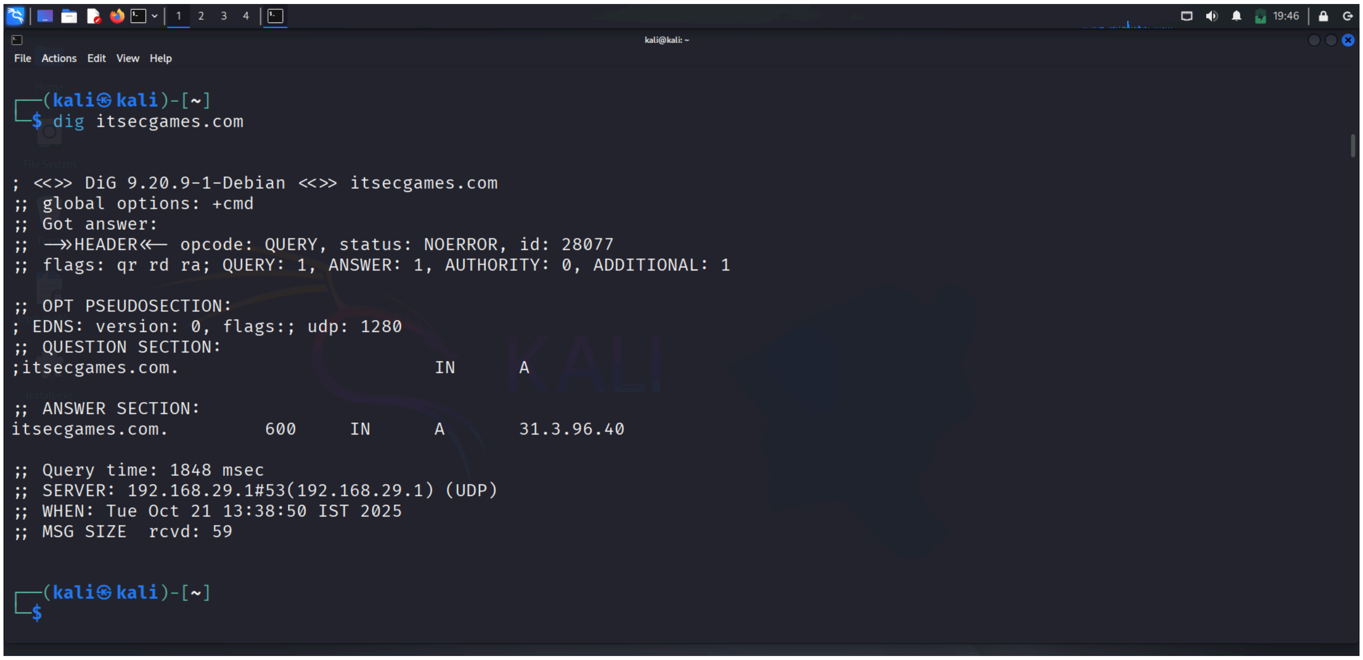
```
┌──(kali㉿kali)-[~]
└─$ dig itsecgames.com MX


; <<>> DiG 9.20.9-1-Debian <<>> itsecgames.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11671
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;itsecgames.com.                        IN      MX

;; ANSWER SECTION:
itsecgames.com.         3600    IN      MX      5 itsecgames-
com.mail.protection.outlook.com.

;; Query time: 176 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Tue Oct 21 13:40:25 IST 2025
;; MSG SIZE  rcvd: 98
```

```
┌──(kali㉿kali)-[~]
└─$ dig itsecgames.com NS


; <<>> DiG 9.20.9-1-Debian <<>> itsecgames.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39798
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;itsecgames.com.                        IN      NS

;; ANSWER SECTION:
itsecgames.com.         3600    IN      NS      ns53.domaincontrol.com.
itsecgames.com.         3600    IN      NS      ns54.domaincontrol.com.

;; Query time: 196 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Tue Oct 21 13:40:45 IST 2025
;; MSG SIZE  rcvd: 95


┌──(kali㉿kali)-[~]
└─$ dig itsecgames.com TXT


; <<>> DiG 9.20.9-1-Debian <<>> itsecgames.com TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3567
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;itsecgames.com.                        IN      TXT

;; ANSWER SECTION:
itsecgames.com.         3600    IN      TXT     "v=spf1 mx a
include:spf.protection.outlook.com include:servers.mcsv.net include:mme-srv-
dc1.mme.local -all"
```

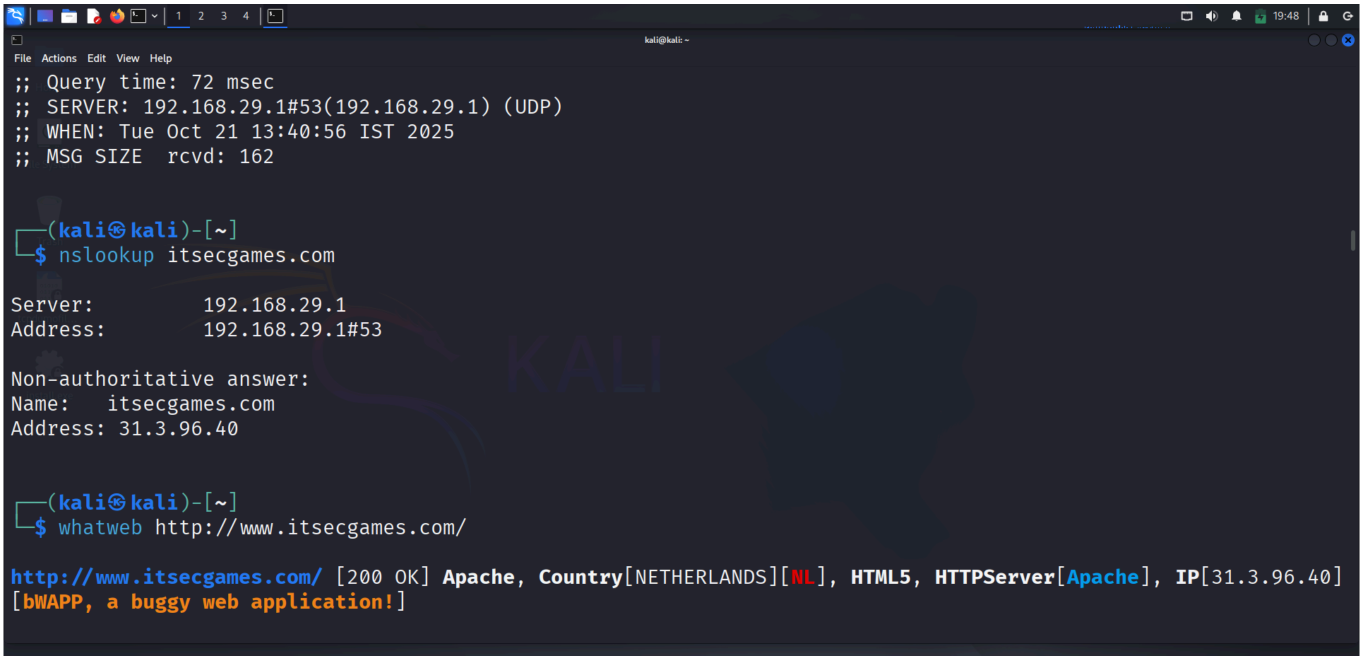
```
;; Query time: 72 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Tue Oct 21 13:40:56 IST 2025
;; MSG SIZE  rcvd: 162
```

NSLOOKUP :

```
┌──(kali㉿kali)-[~]
└─$ nslookup itsecgames.com

Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   itsecgames.com
Address: 31.3.96.40
```



```
┌──(kali㉿kali)-[~]
└─$ dig itsecgames.com

; <<>> DiG 9.20.9-1-Debian <<>> itsecgames.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28077
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;itsecgames.com.                IN      A

;; ANSWER SECTION:
itsecgames.com.         600     IN      A       31.3.96.40

;; Query time: 1848 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Tue Oct 21 13:38:50 IST 2025
;; MSG SIZE  rcvd: 59

┌──(kali㉿kali)-[~]
└─$
```

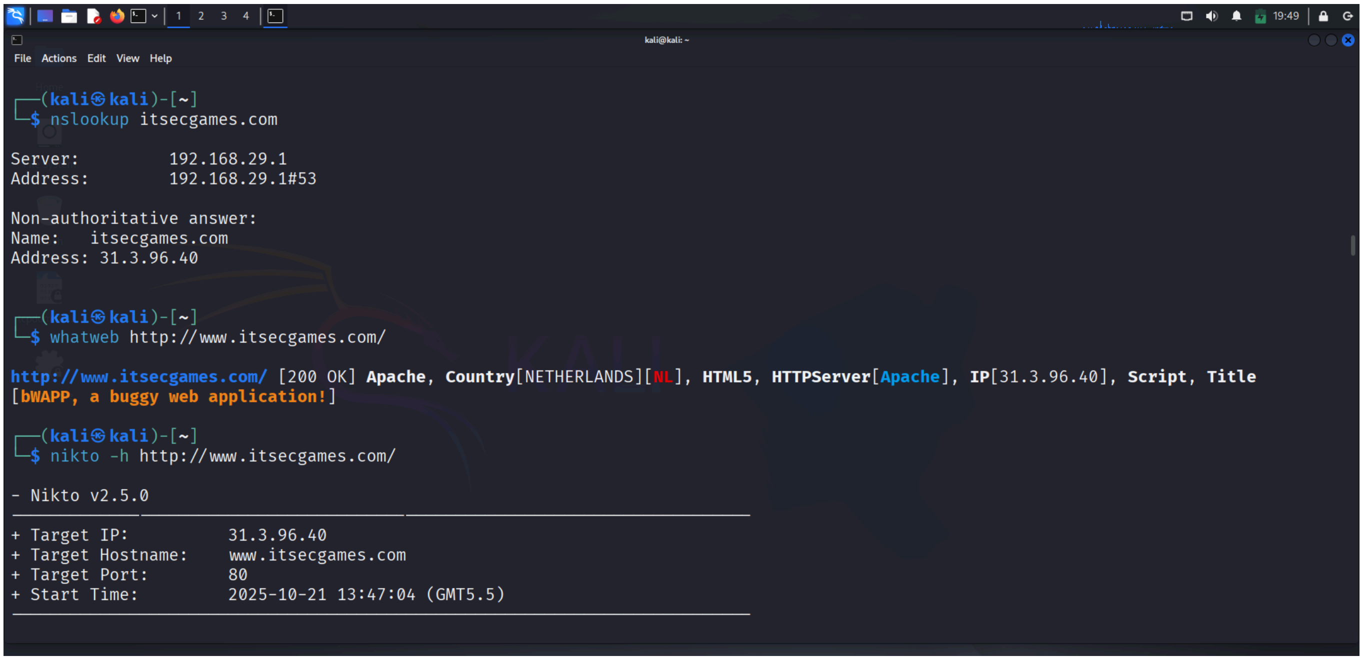


```
;; Query time: 72 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Tue Oct 21 13:40:56 IST 2025
;; MSG SIZE  rcvd: 162


┌──(kali㉿kali)-[~]
└─$ nslookup itsecgames.com

Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   itsecgames.com
Address: 31.3.96.40


┌──(kali㉿kali)-[~]
└─$ whatweb http://www.itsecgames.com/

http://www.itsecgames.com/ [200 OK] Apache, Country[NETHERLANDS][NL], HTML5, HTTPServer[Apache], IP[31.3.96.40]
[bWAPP, a buggy web application!]
```

- IP `31.3.96.40`, MX pointing to Office365, DNS managed by GoDaddy.
- SPF records configured, no DNSSEC.

Technology Fingerprinting:

```
┌──(kali㉿kali)-[~]
└─$ whatweb http://www.itsecgames.com/

http://www.itsecgames.com/ [200 OK] Apache, Country[NETHERLANDS][NL], HTML5,
HTTPServer[Apache], IP[31.3.96.40], Script, Title[bWAPP, a buggy web
application!]
```



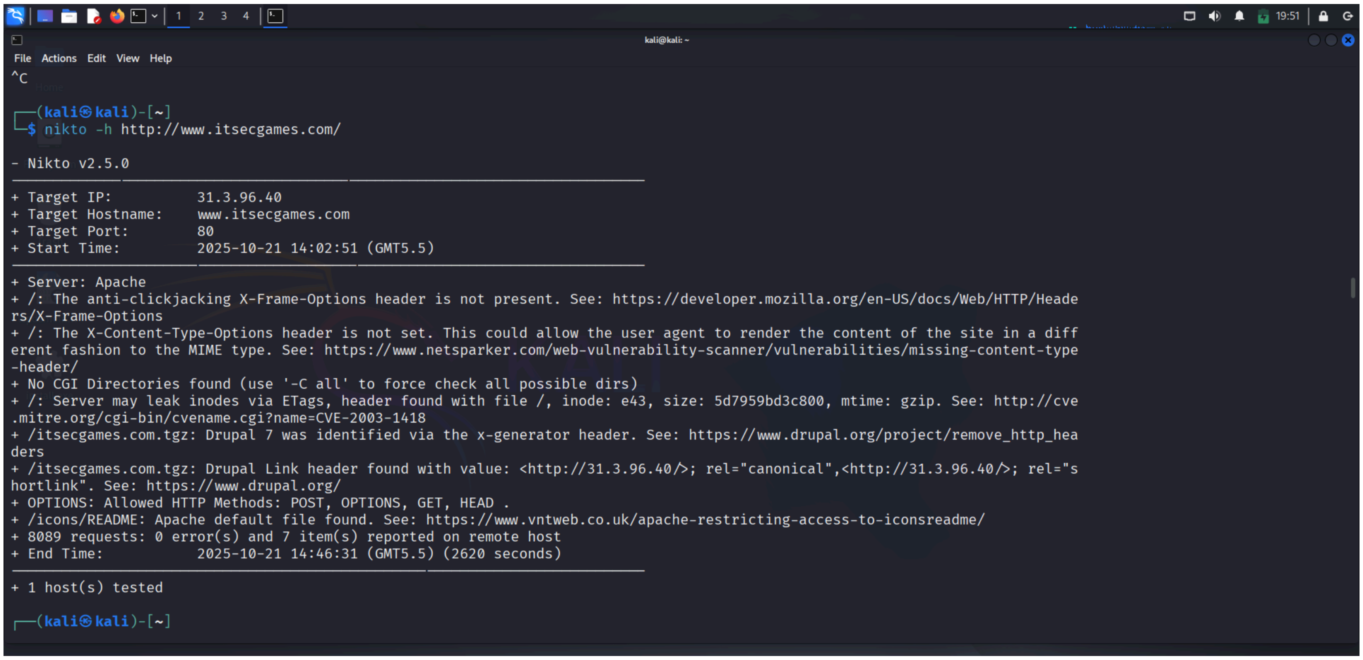
```
┌──(kali㉿kali)-[~]
└─$ nslookup itsecgames.com

Server:         192.168.29.1
Address:        192.168.29.1#53

Non-authoritative answer:
Name:   itsecgames.com
Address: 31.3.96.40


┌──(kali㉿kali)-[~]
└─$ whatweb http://www.itsecgames.com/

http://www.itsecgames.com/ [200 OK] Apache, Country[NETHERLANDS][NL], HTML5, HTTPServer[Apache], IP[31.3.96.40], Script, Title
[bWAPP, a buggy web application!]

┌──(kali㉿kali)-[~]
└─$ nikto -h http://www.itsecgames.com/

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    www.itsecgames.com
+ Target Port:        80
+ Start Time:         2025-10-21 13:47:04 (GMT5.5)
---------------------------------------------------------------------------
```

- Web server: Apache HTTP Server in Netherlands.
- Application: bWAPP (PHP/MySQL training app).
- JavaScript: html5shiv for IE compatibility.

4.2 Vulnerability Scanning

- Nikto Scan:

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://www.itsecgames.com/

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    www.itsecgames.com
+ Target Port:        80
+ Start Time:         2025-10-21 14:02:51 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: e43,
size: 5d7959bd3c800, mtime: gzip. See: http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2003-1418
+ /itsecgames.com.tgz: Drupal 7 was identified via the x-generator header.
See: https://www.drupal.org/project/remove_http_headers
+ /itsecgames.com.tgz: Drupal Link header found with value:
<http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink".
See: https://www.drupal.org/
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /icons/README: Apache default file found. See:
https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8089 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2025-10-21 14:46:31 (GMT5.5) (2620 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



```
^C

┌──(kali㉿kali)-[~]
└─$ nikto -h http://www.itsecgames.com/

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          31.3.96.40
+ Target Hostname:    www.itsecgames.com
+ Target Port:        80
+ Start Time:         2025-10-21 14:02:51 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
rs/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
erent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type
-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: e43, size: 5d7959bd3c800, mtime: gzip. See: http://cve
.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /itsecgames.com.tgz: Drupal 7 was identified via the x-generator header. See: https://www.drupal.org/project/remove_http_hea
ders
+ /itsecgames.com.tgz: Drupal Link header found with value: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="s
hortlink". See: https://www.drupal.org/
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8089 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2025-10-21 14:46:31 (GMT5.5) (2620 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
```

- Missing `X-Frame-Options` and `X-Content-Type-Options` headers.
- Leaks inode data via ETags (CVE-2003-1418).
- Drupal 7 version info exposed via archive files.
- Default Apache files accessible (`/icons/README`).
- HTTP methods POST, OPTIONS, GET, HEAD allowed.

Nmap Scan:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln 31.3.96.40

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 14:48 IST
Nmap scan report for web.mmebvba.com (31.3.96.40)
Host is up (0.29s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 6.7p1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       DF059135-2CF5-5441-8F22-E6EF1DEE5F6E    10.0
https://vulners.com/gitee/DF059135-2CF5-5441-8F22-E6EF1DEE5F6E  *EXPLOIT*
|       PACKETSTORM:173661      9.8
https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8
https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-
3AF0523F3807*EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8
```

```
https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-
8064A1575B23*EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8
https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-
E8DB5379A623*EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8
https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-
2DE89F3927EC*EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8
https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-
1EEAFD4B9FF0*EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8
https://vulners.com/githubexploit/0221525F-07F5-5790-912D-
F4B9E2D1B587*EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       CVE-2016-0778   8.1     https://vulners.com/cve/CVE-2016-0778
|       BA3887BD-F579-53B1-A4A4-FF49E953E1C0    8.1
https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-
FF49E953E1C0*EXPLOIT*
|       4FB01B00-F993-5CAF-BD57-D7E290D10C1F    8.1
https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-
D7E290D10C1F*EXPLOIT*
|       055DEFEB-CD2B-5C05-8024-AA3008C76046    8.1
https://vulners.com/gitee/055DEFEB-CD2B-5C05-8024-AA3008C76046  *EXPLOIT*
|       PACKETSTORM:140070      7.8
https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8
https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09
*EXPLOIT*
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888
*EXPLOIT*
|       CVE-2020-15778  7.8     https://vulners.com/cve/CVE-2020-15778
|       CVE-2016-6515   7.8     https://vulners.com/cve/CVE-2016-6515
|       CVE-2016-10012  7.8     https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325   7.8     https://vulners.com/cve/CVE-2015-8325
|       C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    7.8
https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-
0DAF45EEFFE3*EXPLOIT*
|       312165E3-7FD9-5769-BDA3-4129BE9114D6    7.8
https://vulners.com/githubexploit/312165E3-7FD9-5769-BDA3-
4129BE9114D6*EXPLOIT*
|       2E719186-2FED-58A8-A150-762EFBAAA523    7.8
https://vulners.com/gitee/2E719186-2FED-58A8-A150-762EFBAAA523  *EXPLOIT*
|       23CC97BE-7C95-513B-9E73-298C48D74432    7.8
https://vulners.com/githubexploit/23CC97BE-7C95-513B-9E73-
298C48D74432*EXPLOIT*
```

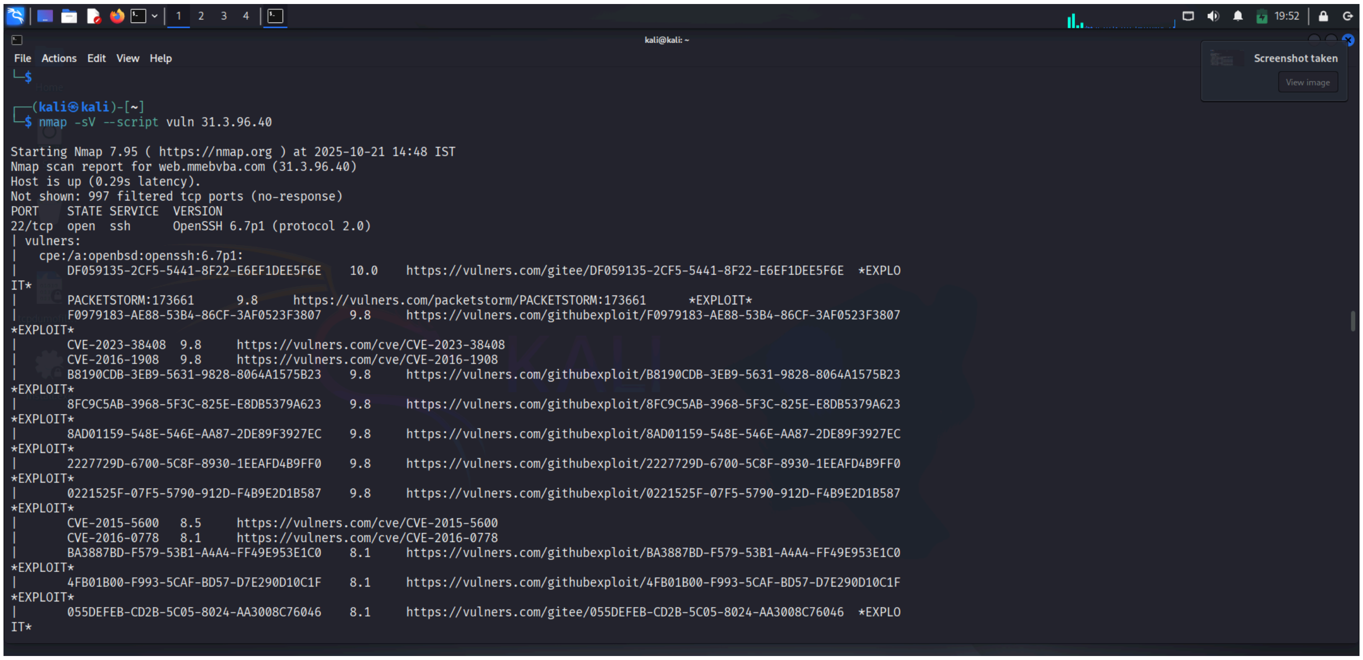
```
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-
26494        *EXPLOIT*
|       10213DBE-F683-58BB-B6D3-353173626207    7.8
https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-
353173626207*EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579
*EXPLOIT*
|       CVE-2016-10708  7.5     https://vulners.com/cve/CVE-2016-10708
|       CVE-2016-10009  7.5     https://vulners.com/cve/CVE-2016-10009
|       CF52FA19-B5DB-5D14-B50F-2411851976E2    7.5
https://vulners.com/githubexploit/CF52FA19-B5DB-5D14-B50F-
2411851976E2*EXPLOIT*
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-
26576        *EXPLOIT*
|       SSV:92582       7.2     https://vulners.com/seebug/SSV:92582
*EXPLOIT*
|       CVE-2021-41617  7.0     https://vulners.com/cve/CVE-2021-41617
|       CVE-2016-10010  7.0     https://vulners.com/cve/CVE-2016-10010
|       284B94FC-FD5D-5C47-90EA-47900DAD1D1E    7.0
https://vulners.com/githubexploit/284B94FC-FD5D-5C47-90EA-
47900DAD1D1E*EXPLOIT*
|       SSV:92580       6.9     https://vulners.com/seebug/SSV:92580
*EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       1337DAY-ID-26577        6.9     https://vulners.com/zdt/1337DAY-ID-
26577        *EXPLOIT*
|       EDB-ID:46516    6.8     https://vulners.com/exploitdb/EDB-ID:46516
*EXPLOIT*
|       EDB-ID:46193    6.8     https://vulners.com/exploitdb/EDB-ID:46193
*EXPLOIT*
|       CVE-2019-6110   6.8     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   6.8     https://vulners.com/cve/CVE-2019-6109
|       1337DAY-ID-32328        6.8     https://vulners.com/zdt/1337DAY-ID-
32328        *EXPLOIT*
|       1337DAY-ID-32009        6.8     https://vulners.com/zdt/1337DAY-ID-
32009        *EXPLOIT*
|       D104D2BF-ED22-588B-A9B2-3CCC562FE8C0    6.5
https://vulners.com/githubexploit/D104D2BF-ED22-588B-A9B2-
3CCC562FE8C0*EXPLOIT*
|       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
|       CVE-2016-0777   6.5     https://vulners.com/cve/CVE-2016-0777
|       C07ADB46-24B8-57B7-B375-9C761F4750A2    6.5
https://vulners.com/githubexploit/C07ADB46-24B8-57B7-B375-
9C761F4750A2*EXPLOIT*
|       A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C    6.5
https://vulners.com/githubexploit/A88CDD3E-67CC-51CC-97FB-
```

```
AB0CACB6B08C*EXPLOIT*
|       65B15AA1-2A8D-53C1-9499-69EBA3619F1C    6.5
https://vulners.com/githubexploit/65B15AA1-2A8D-53C1-9499-
69EBA3619F1C*EXPLOIT*
|       5325A9D6-132B-590C-BDEF-0CB105252732    6.5
https://vulners.com/gitee/5325A9D6-132B-590C-BDEF-0CB105252732  *EXPLOIT*
|       530326CF-6AB3-5643-AA16-73DC8CB44742    6.5
https://vulners.com/githubexploit/530326CF-6AB3-5643-AA16-
73DC8CB44742*EXPLOIT*
|       EDB-ID:40858    6.4     https://vulners.com/exploitdb/EDB-ID:40858
*EXPLOIT*
|       EDB-ID:40119    6.4     https://vulners.com/exploitdb/EDB-ID:40119
*EXPLOIT*
|       EDB-ID:39569    6.4     https://vulners.com/exploitdb/EDB-ID:39569
*EXPLOIT*
|       CVE-2016-3115   6.4     https://vulners.com/cve/CVE-2016-3115
|       PACKETSTORM:181223      5.9
https://vulners.com/packetstorm/PACKETSTORM:181223      *EXPLOIT*
|       MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-        5.9
https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-
*EXPLOIT*
|       EDB-ID:40136    5.9     https://vulners.com/exploitdb/EDB-ID:40136
*EXPLOIT*
|       EDB-ID:40113    5.9     https://vulners.com/exploitdb/EDB-ID:40113
*EXPLOIT*
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2020-14145  5.9     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6111   5.9     https://vulners.com/cve/CVE-2019-6111
|       CVE-2016-6210   5.9     https://vulners.com/cve/CVE-2016-6210
|       A02ABE85-E4E3-5852-A59D-DF288CB8160A    5.9
https://vulners.com/githubexploit/A02ABE85-E4E3-5852-A59D-
DF288CB8160A*EXPLOIT*
|       6D74A425-60A7-557A-B469-1DD96A2D8FF8    5.9
https://vulners.com/githubexploit/6D74A425-60A7-557A-B469-
1DD96A2D8FF8*EXPLOIT*
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8
https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19
*EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8
https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97
*EXPLOIT*
|       SSV:91041       5.5     https://vulners.com/seebug/SSV:91041
*EXPLOIT*
|       PACKETSTORM:140019      5.5
https://vulners.com/packetstorm/PACKETSTORM:140019      *EXPLOIT*
|       PACKETSTORM:136251      5.5
```

```
https://vulners.com/packetstorm/PACKETSTORM:136251      *EXPLOIT*
|       PACKETSTORM:136234      5.5
https://vulners.com/packetstorm/PACKETSTORM:136234      *EXPLOIT*
|       EXPLOITPACK:F92411A645D85F05BDBD274FD222226F    5.5
https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05BDBD274FD222226F
*EXPLOIT*
|       EXPLOITPACK:9F2E746846C3C623A27A441281EAD138    5.5
https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623A27A441281EAD138
*EXPLOIT*
|       EXPLOITPACK:1902C998CBF9154396911926B4C3B330    5.5
https://vulners.com/exploitpack/EXPLOITPACK:1902C998CBF9154396911926B4C3B330
*EXPLOIT*
|       CVE-2016-10011  5.5     https://vulners.com/cve/CVE-2016-10011
|       1337DAY-ID-25388        5.5     https://vulners.com/zdt/1337DAY-ID-
25388        *EXPLOIT*
|       FD18B68B-C0A6-562E-A8C8-781B225F15B0    5.3
https://vulners.com/githubexploit/FD18B68B-C0A6-562E-A8C8-
781B225F15B0*EXPLOIT*
|       EDB-ID:45939    5.3     https://vulners.com/exploitdb/EDB-ID:45939
*EXPLOIT*
|       EDB-ID:45233    5.3     https://vulners.com/exploitdb/EDB-ID:45233
*EXPLOIT*
|       E9EC0911-E2E1-52A7-B2F4-D0065C6A3057    5.3
https://vulners.com/githubexploit/E9EC0911-E2E1-52A7-B2F4-
D0065C6A3057*EXPLOIT*
|       CVE-2018-20685  5.3     https://vulners.com/cve/CVE-2018-20685
|       CVE-2018-15919  5.3     https://vulners.com/cve/CVE-2018-15919
|       CVE-2018-15473  5.3     https://vulners.com/cve/CVE-2018-15473
|       CVE-2017-15906  5.3     https://vulners.com/cve/CVE-2017-15906
|       CVE-2016-20012  5.3     https://vulners.com/cve/CVE-2016-20012
|       A9E6F50E-E7FC-51D0-9C93-A43461469FA2    5.3
https://vulners.com/githubexploit/A9E6F50E-E7FC-51D0-9C93-
A43461469FA2*EXPLOIT*
|       A801235B-9835-5BA8-B8FE-23B7FFCABD66    5.3
https://vulners.com/githubexploit/A801235B-9835-5BA8-B8FE-
23B7FFCABD66*EXPLOIT*
|       8DD1D813-FD5A-5B26-867A-CE7CAC9FEEDF    5.3
https://vulners.com/gitee/8DD1D813-FD5A-5B26-867A-CE7CAC9FEEDF  *EXPLOIT*
|       486BB6BC-9C26-597F-B865-D0E904FDA984    5.3
https://vulners.com/githubexploit/486BB6BC-9C26-597F-B865-
D0E904FDA984*EXPLOIT*
|       2385176A-820F-5469-AB09-C340264F2B2F    5.3
https://vulners.com/gitee/2385176A-820F-5469-AB09-C340264F2B2F  *EXPLOIT*
|       1337DAY-ID-31730        5.3     https://vulners.com/zdt/1337DAY-ID-
31730        *EXPLOIT*
|       SSH_ENUM        5.0     https://vulners.com/canvas/SSH_ENUM
```

```
*EXPLOIT*
|       PACKETSTORM:150621      5.0
https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
|       EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    5.0
https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0
*EXPLOIT*
|       EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    5.0
https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283
*EXPLOIT*
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447
*EXPLOIT*
|       EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF    4.3
https://vulners.com/exploitpack/EXPLOITPACK:802AF3229492E147A5F09C7F2B27C6DF
*EXPLOIT*
|       EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF    4.3
https://vulners.com/exploitpack/EXPLOITPACK:5652DDAA7FE452E19AC0DC1CD97BA3EF
*EXPLOIT*
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       1337DAY-ID-25440        4.3     https://vulners.com/zdt/1337DAY-ID-
25440        *EXPLOIT*
|       1337DAY-ID-25438        4.3     https://vulners.com/zdt/1337DAY-ID-
25438        *EXPLOIT*
|       CVE-2021-36368  3.7     https://vulners.com/cve/CVE-2021-36368
|       CVE-2025-61985  3.6     https://vulners.com/cve/CVE-2025-61985
|       CVE-2025-61984  3.6     https://vulners.com/cve/CVE-2025-61984
|       B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150    3.6
https://vulners.com/githubexploit/B7EACB4F-A5CF-5C5A-809F-
E03CCE2AB150*EXPLOIT*
|       4C6E2182-0E99-5626-83F6-1646DD648C57    3.6
https://vulners.com/githubexploit/4C6E2182-0E99-5626-83F6-
1646DD648C57*EXPLOIT*
|       SSV:92581       2.1     https://vulners.com/seebug/SSV:92581
*EXPLOIT*
|       CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
|       PACKETSTORM:151227      0.0
https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|       PACKETSTORM:140261      0.0
https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
|       PACKETSTORM:138006      0.0
https://vulners.com/packetstorm/PACKETSTORM:138006      *EXPLOIT*
|       PACKETSTORM:137942      0.0
https://vulners.com/packetstorm/PACKETSTORM:137942      *EXPLOIT*
|       1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-
30937        *EXPLOIT*
|       1337DAY-ID-26468        0.0     https://vulners.com/zdt/1337DAY-ID-
26468        *EXPLOIT*
```

```
|_      1337DAY-ID-25391        0.0     https://vulners.com/zdt/1337DAY-ID-
25391        *EXPLOIT*
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp open  ssl/http Apache httpd
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 405.73 seconds
```



```
└─$

┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln 31.3.96.40

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 14:48 IST
Nmap scan report for web.mmebvba.com (31.3.96.40)
Host is up (0.29s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 6.7p1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       DF059135-2CF5-5441-8F22-E6EF1DEE5F6E    10.0    https://vulners.com/gitee/DF059135-2CF5-5441-8F22-E6EF1DEE5F6E  *EXPLO
IT*
|       PACKETSTORM:173661      9.8     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807
*EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23
*EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623
*EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC
*EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0
*EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587
*EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       CVE-2016-0778   8.1     https://vulners.com/cve/CVE-2016-0778
|       BA3887BD-F579-53B1-A4A4-FF49E953E1C0    8.1     https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-FF49E953E1C0
*EXPLOIT*
|       4FB01B00-F993-5CAF-BD57-D7E290D10C1F    8.1     https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F
*EXPLOIT*
|       055DEFEB-CD2B-5C05-8024-AA3008C76046    8.1     https://vulners.com/gitee/055DEFEB-CD2B-5C05-8024-AA3008C76046  *EXPLO
IT*
```

- SSH (port 22) running OpenSSH 6.7p1, multiple critical vulnerabilities (e.g., CVE-2023-38408).
- Web server on ports 80 and 443 Apache with moderate info disclosures; no scripted XSS or CSRF detected.

4.3 SSL/TLS Configuration

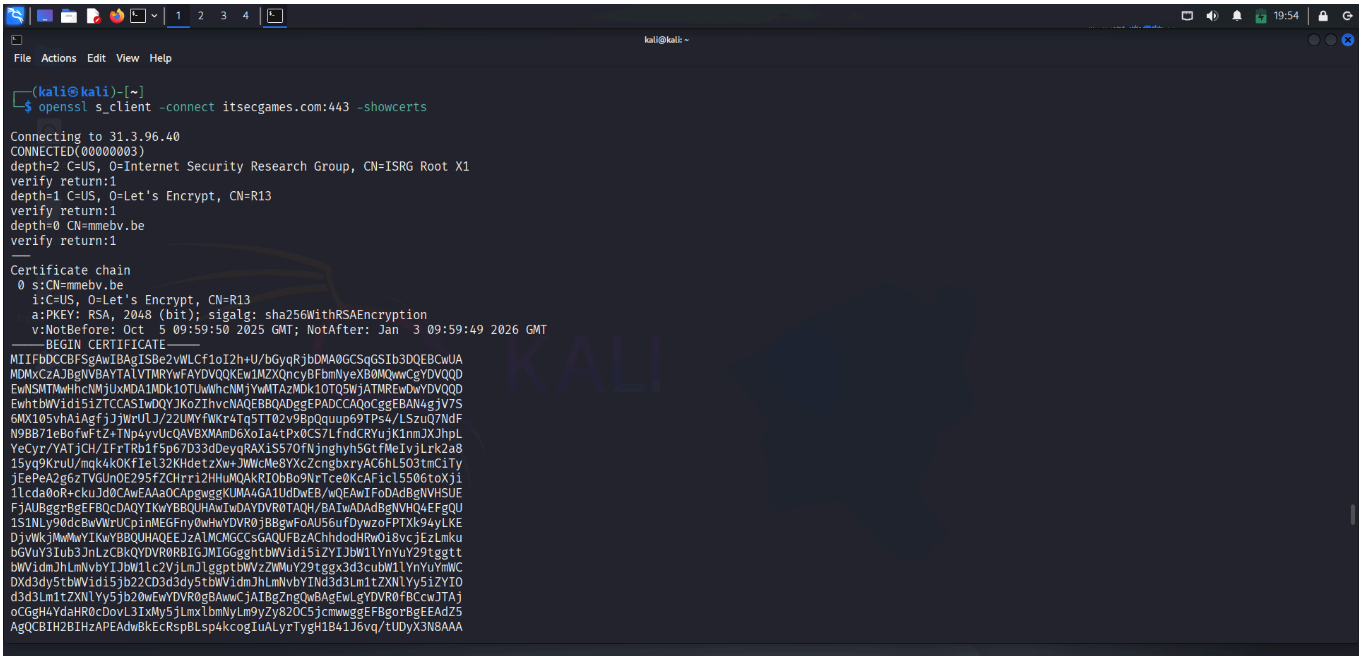
- **OpenSSL SSL Client:**

```
┌──(kali㉿kali)-[~]
└─$ openssl s_client -connect itsecgames.com:443 -showcerts

Connecting to 31.3.96.40
CONNECTED(00000003)
depth=2 C=US, O=Internet Security Research Group, CN=ISRG Root X1
verify return:1
depth=1 C=US, O=Let's Encrypt, CN=R13
verify return:1
depth=0 CN=mmebv.be
verify return:1
---
Certificate chain
 0 s:CN=mmebv.be
   i:C=US, O=Let's Encrypt, CN=R13
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Oct  5 09:59:50 2025 GMT; NotAfter: Jan  3 09:59:49 2026 GMT
-----BEGIN CERTIFICATE-----
MIIFbDCCBFSgAwIBAgISBe2vWLCf1oI2h+U/bGyqRjbDMA0GCSqGSIb3DQEBCwUA
MDMxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQwwCgYDVQQD
EwNSMTMwHhcNMjUxMDA1MDk1OTUwWhcNMjYwMTAzMDk1OTQ5WjATMREwDwYDVQQD
EwhtbWVidi5iZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN4gjV7S
6MX105vhAiAgfjJjWrUlJ/22UMYfWKr4Tq5TT02v9BpQquup69TPs4/LSzuQ7NdF
N9BB71eBofwFtZ+TNp4yvUcQAVBXMAmD6XoIa4tPx0CS7LfndCRYujK1nmJXJhpL
YeCyr/YATjCH/IFrTRb1f5p67D33dDeyqRAXiS57OfNjnghyh5GtfMeIvjLrk2a8
15yq9KruU/mqk4kOKfIel32KHdetzXw+JWWcMe8YXcZcngbxryAC6hL5O3tmCiTy
jEePeA2g6zTVGUnOE295fZCHrri2HHuMQAkRIObBo9NrTce0KcAFicl5506toXji
1lcda0oR+ckuJd0CAwEAAaOCApgwggKUMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUE
FjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU
1S1NLy90dcBwVWrUCpinMEGFny0wHwYDVR0jBBgwFoAU56ufDywzoFPTXk94yLKE
DjvWkjMwMwYIKwYBBQUHAQEEJzAlMCMGCCsGAQUFBzAChhdodHRwOi8vcjEzLmku
bGVuY3Iub3JnLzCBkQYDVR0RBIGJMIGGghtbWVidi5iZYIJbW1lYnYuY29tggtt
bWVidmJhLmNvbYIJbW1lc2VjLmJlggptbWVzZWMuY29tggx3d3cubW1lYnYuYmWC
DXd3dy5tbWVidi5jb22CD3d3dy5tbWVidmJhLmNvbYINd3d3Lm1tZXNlYy5iZYIO
d3d3Lm1tZXNlYy5jb20wEwYDVR0gBAwwCjAIBgZngQwBAgEwLgYDVR0fBCcwJTAj
oCGgH4YdaHR0cDovL3IxMy5jLmxlbmNyLm9yZy82OC5jcmwwggEFBgorBgEEAdZ5
AgQCBIH2BIHzAPEAdwBkEcRspBLsp4kcogIuALyrTygH1B41J6vq/tUDyX3N8AAA
AZm0BcMdAAAEAwBIMEYCIQDf2bsjmQSxH+Hfeke1Dduu+hvKGF912Dm5zVhakMSF
vQIhAIT6hxVhYrE5iyB17ztnrtngzBYzSEy+H0jyOKXVZjqnAHYAlpdkv1VYl633
Q4doNwhCd+nwOtX2pPM2bkakPw/KqcYAAAGZtAXLOgAABAMARzBFAiEAgtahjos4
9lPaS5cDYpn1kxqWCWRsmresQs6rH0mSS6cCIHpD49LI6HzelNadSBFJRqja52rO
FbqeMkMJtuFmxj0CMA0GCSqGSIb3DQEBCwUAA4IBAQBR+Eh10o4oY7Aq4DSOYebI
Ejc5/xVJzWRgjNYpzTgdM4CKj75ObWlqCuQ2HtLLxbUBnquv/TKiRpi98KCW1keq
NK3ejYPQagQdjxtmEMP6Uo0Qy9VFpieVjC0oxgQ+OybZjerMQDYawPdanA52RQfS
```

```
UzsVd7hAEqllsNYLzgYFt8XmcNIccVU/6cGVdfE5Xmsym9WO3UKNVSA7x2fNQttc
Zd+Zl47ltBUg51byJ1p3pkkzwIN5B2TNhtjRWFcKMQlZXcmuWQ9QymFafJfhTVK+
H53KPENcw3Udn10m6OnLBdDusPmowB+Mi+CGTVm+EOMXcP7BFXEY2C0TSnVMeIX7
-----END CERTIFICATE-----
 1 s:C=US, O=Let's Encrypt, CN=R13
   i:C=US, O=Internet Security Research Group, CN=ISRG Root X1
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
-----BEGIN CERTIFICATE-----
MIIFBTCCAu2gAwIBAgIQWgDyEtjUtIDzkkFX6imDBTANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEpMCcGA1UEChMgSW50ZXJuZXQgU2VjdXJpdHkgUmVzZWFy
Y2ggR3JvdXAxFTATBgNVBAMTDElTUkcgUm9vdCBYMTAeFw0yNDAzMTMwMDAwMDBa
Fw0yNzAzMTIyMzU5NTlaMDMxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBF
bmNyeXB0MQwwCgYDVQQDEwNSMTMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQClZ3CN0FaBZBUXYc25BtStGZCMJlA3mBZjklTb2cyEBZPs0+wIG6BgUUNI
fSvHSJaetC3ancgnO1ehn6vw1g7UDjDKb5ux0daknTI+WE41b0VYaHEX/D7YXYKg
L7JRbLAaXbhZzjVlyIuhrxA3/+OcXcJJFzT/jCuLjfC8cSyTDB0FxLrHzarJXnzR
yQH3nAP2/Apd9Np75tt2QnDr9E0i2gB3b9bJXxf92nUupVcM9upctuBzpWjPoXTi
dYJ+EJ/B9aLrAek4sQpEzNPCifVJNYIKNLMc6YjCR06CDgo28EdPivEpBHXazeGa
XP9enZiVuppD0EqiFwUBBDDTMrOPAgMBAAGjgfgwgfUwDgYDVR0PAQH/BAQDAgGG
MB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATASBgNVHRMBAf8ECDAGAQH/
AgEAMB0GA1UdDgQWBBTnq58PLDOgU9NeT3jIsoQOO9aSMzAfBgNVHSMEGDAWgBR5
tFnme7bl5AFzgAiIyBpY9umbbjAyBggrBgEFBQcBAQQmMCQwIgYIKwYBBQUHMAKG
Fmh0dHA6Ly94MS5pLmxlbmNyLm9yZy8wEwYDVR0gBAwwCjAIBgZngQwBAgEwJwYD
VR0fBCAwHjAcoBqgGIYWaHR0cDovL3gxLmMubGVuY3Iub3JnLzANBgkqhkiG9w0B
AQsFAAOCAgEAUTdYUqEimzW7TbrOypLqCfL7VOwYf/Q79OH5cHLCZeggfQhDconl
k7Kgh8b0vi+/XuWu7CN8n/UPeg1vo3G+taXirrytthQinAHGwc/UdbOygJa9zuBc
VyqoH3CXTXDInT+8a+c3aEVMJ2St+pSn4ed+WkDp8ijsijvEyFwE47hulW0Ltzjg
9fOV5Pmrg/zxWbRuL+k0DBDHEJennCsAen7c35Pmx7jpmJ/HtgRhcnz0yjSBvyIw
6L1QIupkCv2SBODT/xDD3gfQQyKv6roV4G2EhfEyAsWpmojxjCUCGiyg97FvDtm/
NK2LSc9lybKxB73I2+P2G3CaWpvvpAiHCVu30jW8GCxKdfhsXtnIy2imskQqVZ2m
0Pmxobb28Tucr7xBK7CtwvPrb79os7u2XP3O5f9b/H66GNyRrglRXlrYjI1oGYL/
f4I1n/Sgusda6WvA6C190kxjU15Y12mHU4+BxyR9cx2hhGS9fAjMZKJss28qxvz6
Axu4CaDmRNZpK/pQrXF17yXCXkmEWgvSOEZy6Z9pcbLIVEGckV/iVeq0AOo2pkg9
p4QRIy0tK2diRENLSF2KysFwbY6B26BFeFs3v1sYVRhFW9nLkOrQVporCS0KyZmf
wVD89qSTlnctLcZnIavjKsKUu1nA1iU0yYMdYepKR7lWbnwhdx3ewok=
-----END CERTIFICATE-----
---
Server certificate
subject=CN=mmebv.be
issuer=C=US, O=Let's Encrypt, CN=R13
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: rsa_pkcs1_sha256
Peer Temp Key: ECDH, prime256v1, 256 bits
```

```
---
SSL handshake has read 3390 bytes and written 1809 bytes
Verification: OK
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Protocol: TLSv1.2
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID:
688B078A5FADA17DA3F1C32EADC0FA7A5888B0F6F418FABA5A6D83E5D101FCD1
    Session-ID-ctx:
    Master-Key:
D8E70FA03407B1EA22C2E3CEB37A28411D4FA0FA0BF65DF2983AACE915238A97C0D87A8CAB0B9B
0E62EA2511F9B19581
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 27 b5 ec 39 8e 1b 91 09-7d b3 8d 45 95 8a 88 54   '..9....}..E...T
    0010 - d3 8d 8d 33 5b ba a9 0b-c4 c2 5a 67 3b 32 06 b3   ...3[.....Zg;2..
    0020 - 3b 63 57 31 45 4f 8c 1b-3d 61 cd ea 81 7d 01 c4   ;cW1EO..=a...}..
    0030 - 4a e7 19 8d ef 5c 2d 65-c5 44 61 86 53 50 ef 11   J....\-e.Da.SP..
    0040 - b0 23 a4 ad 9c 07 e4 36-d3 b3 57 0b db 9c bb 8c   .#.....6..W.....
    0050 - 61 41 9a f0 74 97 5d 81-ac e4 97 64 a6 23 aa f1   aA..t.]....d.#..
    0060 - 87 7c 7c 87 a7 9c 63 1c-00 59 a3 41 31 1b f6 ac   .||...c..Y.A1...
    0070 - 83 98 5a 8f eb 39 04 24-92 3e a5 71 42 47 1a 9d   ..Z..9.$.>.qBG..
    0080 - 63 ca b5 56 00 72 95 42-92 74 99 dd db 8c 54 c4   c..V.r.B.t....T.
    0090 - 44 7c e7 be cb b0 4d 0e-22 8f cf cc d3 a0 33 ef   D|....M.".....3.
    00a0 - 41 90 8b bd 0d 7f ae dc-60 f1 26 b1 bc e5 ae b0   A.......`.&.....
    00b0 - b9 0f 30 f6 ba e9 5a db-e6 eb 2f 93 a2 5f 9b 97   ..0...Z.../.._..
    00c0 - 7a 5c 6b 38 e2 d7 ab 80-28 2a d6 37 b7 8b 7e ff   z\k8....(*.7..~.

    Start Time: 1761038857
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
---
40C7248EEF7F0000:error:0A000126:SSL routines::unexpected eof while
```

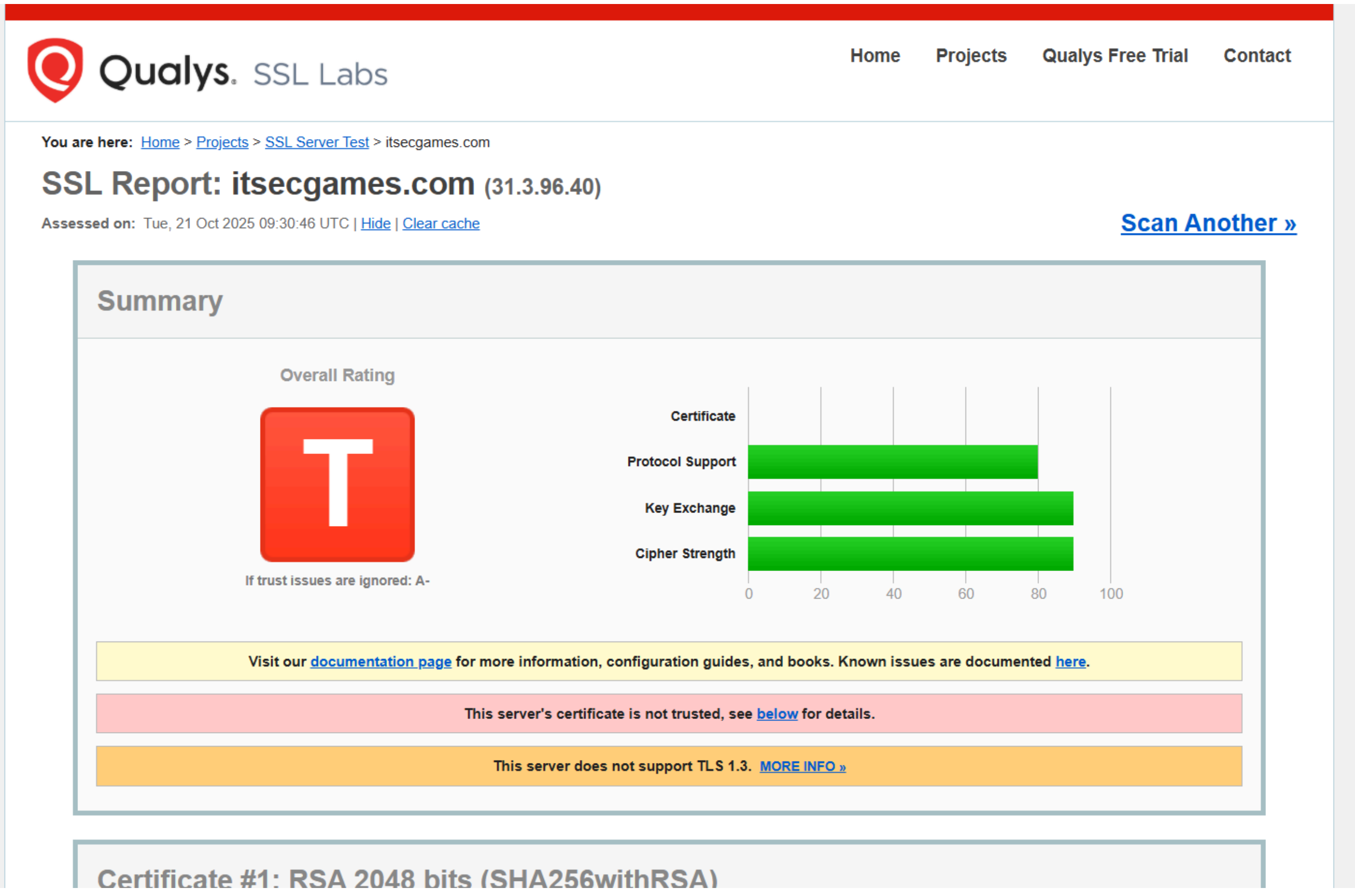
```
reading:../ssl/record/rec_layer_s3.c:691:
```



```
┌──(kali㉿kali)-[~]
└─$ openssl s_client -connect itsecgames.com:443 -showcerts

Connecting to 31.3.96.40
CONNECTED(00000003)
depth=2 C=US, O=Internet Security Research Group, CN=ISRG Root X1
verify return:1
depth=1 C=US, O=Let's Encrypt, CN=R13
verify return:1
depth=0 CN=mmebv.be
verify return:1
---
Certificate chain
 0 s:CN=mmebv.be
   i:C=US, O=Let's Encrypt, CN=R13
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Oct  5 09:59:50 2025 GMT; NotAfter: Jan  3 09:59:49 2026 GMT
-----BEGIN CERTIFICATE-----
MIIFbDCCBFSgAwIBAgISBe2vWLCf1oI2h+U/bGyqRjbDMA0GCSqGSIb3DQEBCwUA
MDMxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQwwCgYDVQQD
EwNSMTMwHhcNMjUxMDA1MDk1OTUwWhcNMjYwMTAzMDk1OTQ5WjATMREwDwYDVQQD
EwhtbWVidi5iZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAN4gjV7S
6MX105vhAiAgfjJjWrUlJ/22UMYfWKr4Tq5TT02v9BpQquup69TPs4/LSzuQ7NdF
N9BB71eBofwFtZ+TNp4yvUcQAVBXMAmD6XoIa4tPx0CS7LfndCRYujK1nmJXJhpL
YeCyr/YATjCH/IFrTRb1f5p67D33dDeyqRAXiS57OfNjnghyh5GtfMeIvjLrk2a8
15yq9KruU/mqk4kOKfIel32KHdetzXw+JWWcMe8YXcZcngbxryAC6hL5O3tmCiTy
jEePeA2g6zTVGUnOE295fZCHrri2HHuMQAkRIObBo9NrTce0KcAFicl5506toXji
1lcda0oR+ckuJd0CAwEAAaOCApgwggKUMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUE
FjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU
1S1NLy90dcBwVWrUCpinMEGFny0wHwYDVR0jBBgwFoAU56ufDywzoFPTXk94yLKE
DjvWkjMwMwYIKwYBBQUHAQEEJzAlMCMGCCsGAQUFBzAChhdodHRwOi8vcjEzLmku
bGVuY3Iub3JnLzCBkQYDVR0RBIGJMIGGghtbWVidi5iZYIJbW1lYnYuY29tggtt
bWVidmJhLmNvbYIJbW1lc2VjLmJlggptbWVzZWMuY29tggx3d3cubW1lYnYuYmWC
DXd3dy5tbWVidi5jb22CD3d3dy5tbWVidmJhLmNvbYINd3d3Lm1tZXNlYy5iZYIO
d3d3Lm1tZXNlYy5jb20wEwYDVR0gBAwwCjAIBgZngQwBAgEwLgYDVR0fBCcwJTAj
oCGgH4YdaHR0cDovL3IxMy5jLmxlbmNyLm9yZy82OC5jcmwwggEFBgorBgEEAdZ5
AgQCBIH2BIHzAPEAdwBkEcRspBLsp4kcogIuALyrTygH1B41J6vq/tUDyX3N8AAA
```

- TLS 1.2 supported with strong ECDHE_RSA_A256 cipher suite.
- Certificate valid until Jan 2026, issued by Let's Encrypt.

Qualys SSL Labs:



You are here: Home > Projects > SSL Server Test > itsecgames.com

SSL Report: itsecgames.com (31.3.96.40)

Assessed on: Tue, 21 Oct 2025 09:30:46 UTC | Hide | Clear cache

Summary

Overall Rating

If trust issues are ignored: A-

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

This server does not support TLS 1.3. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

- Certificate expired recently (May 2025), causing trust errors.
- Missing HSTS header and OCSP stapling.
- No TLS 1.3 support.

5. Prioritized Findings and Recommendations

Priority	Finding	Recommendation
High	Multiple critical OpenSSH CVEs on port 22	Upgrade OpenSSH; restrict and monitor SSH access
Medium	Expired SSL certificate	Renew SSL certificate with trusted CA
Medium	Missing security headers	AddX-Frame-Options,X-Content-Type-Options,HSTSheaders
Medium	Information leakage (Apache defaults, Drupal headers)	Harden Apache config; remove defaults and obfuscate headers
Low	DNSSEC not implemented	Implement DNSSEC for DNS integrity
Low	TLS 1.3 not supported	Upgrade SSL/TLS protocols for modern standards

6. Conclusion

The assessment comprehensively identified vulnerabilities and configuration weaknesses affecting `itsecgames.com`. Critical SSH vulnerabilities and expired SSL certificates present significant security risks and should be remediated immediately. Medium-priority improvements in HTTP headers and web server hardening will reduce the attack surface. This detailed report fulfills the problem statement requirements with actionable insights.

1. **Identify vulnerabilities on the domain:**
   The report includes detailed findings from Nikto and Nmap scans which identified vulnerabilities such as missing security headers, exposed files, and critically vulnerable OpenSSH 6.7 running on port 22 with multiple CVEs.
2. **Detect potential vulnerabilities (misconfigurations, outdated software, CVEs):**
   The report highlights misconfigurations like missing HTTP security headers (`X-Frame-Options`, `X-Content-Type-Options`), exposed Apache default files, Drupal version disclosures, and outdated SSH software with known CVEs that pose security risks.

   Critical vulnerabilities:
   The SSH service running OpenSSH 6.7p1 on port 22 contains multiple critical known CVEs exposing it to remote exploitation, including but not limited to:
   - CVE-2023-38408

- CVE-2016-1908
- CVE-2015-5600
- CVE-2016-0778
- CVE-2020-15778
  These require immediate patching and access restrictions.

3. **Assess SSL/TLS configuration and certificate health:**
   You have a dedicated section covering SSL/TLS analysis done via OpenSSL and SSL Labs, noting an expired Let’s Encrypt certificate, supported protocols (TLS 1.2), lack of TLS 1.3, missing HSTS and OCSP stapling, along with the overall security posture.
4. **Highlight exposed information that could aid attackers:**
   Exposed server banners, headers, HTTP methods, and error pages have been identified and summarized, showing possible information leaks that attackers could leverage.
5. **Provide a prioritized list of findings with mitigation recommendations:**
   Priority categorization is clear, with critical, medium, and low priority findings, accompanied by specific recommended remediations such as upgrading SSH, renewing certificates, adding important HTTP headers, and implementing DNSSEC.