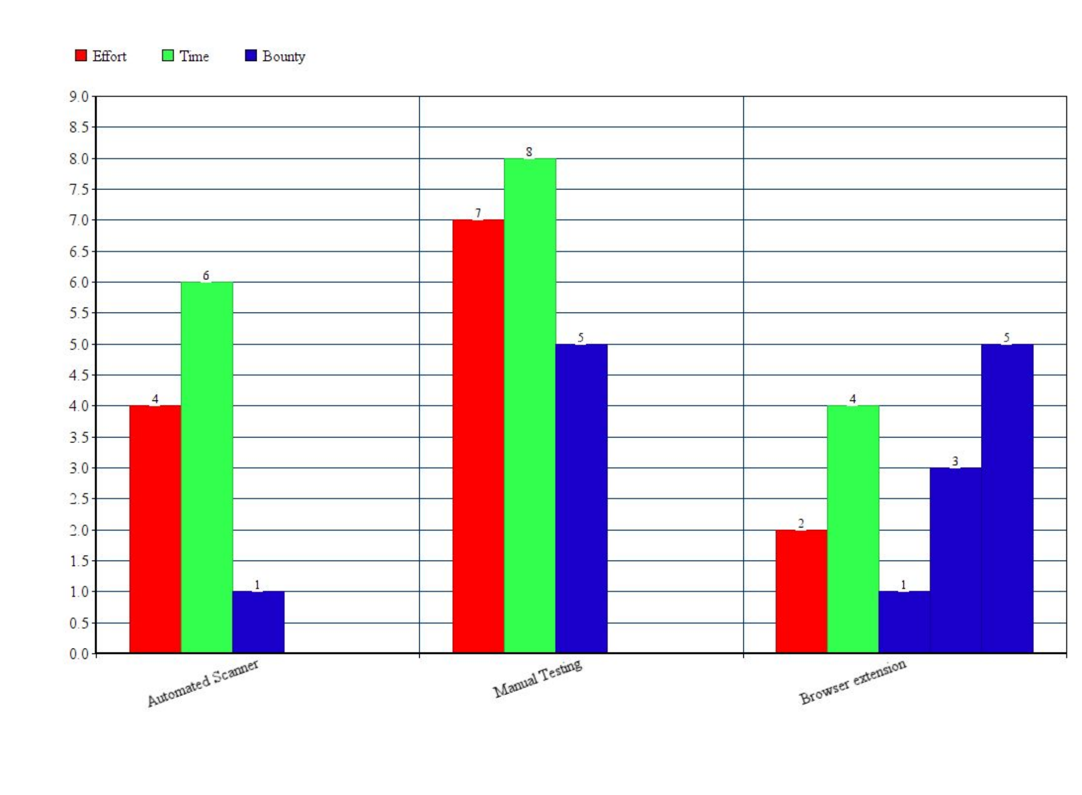
Creating custom browser extensions

...

whoami

- Rewanth Cool - @Rewanth_Cool
- Full stack developer
- Open source contributor
- Penetration tester
- Bug bounty hunter
- CTF player
- Event organizer

Comparison Sheet



What this talk is about

- Low hanging fruits
  - CORS
  - Host header injection
  - Clickjacking
- Firefox extension to detect above vulnerabilities

BASICS FIRST

We will discuss all vulnerabilities in simple **WEBD** terms.

W*hat it is ?*

E*xploitability*

B*iggest Bounties*

D*etection*

CORS Misconfiguration

W - Gives permissions to load scripts/request resources from other pages/domains.

E - If the website allows loading scripts, then attackers will be able to exploit it.

B - https://hackerone.com/reports/235200 ($1000)

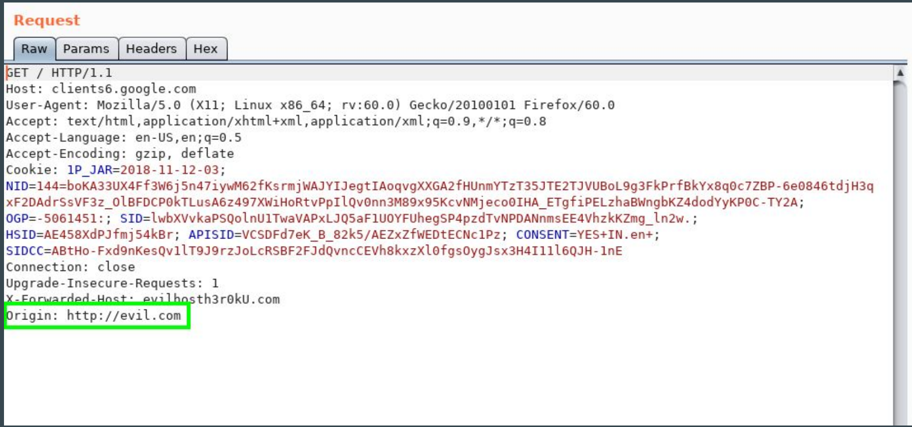
D - $(curl -I URL -H “Origin: evil.com”)

CORS Misconfiguration (Cont..,)

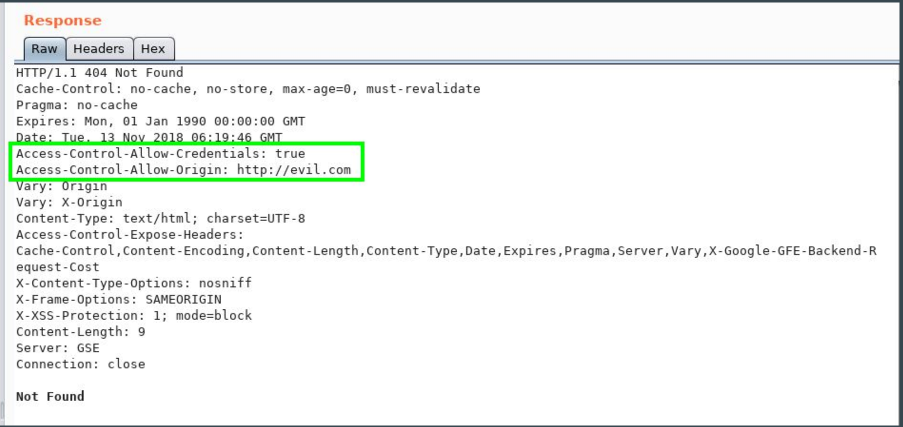
Request headers - Origin: evil.com

Access-Control-Allow-Origin: (http://evil.com || * || null)

Access-Control-Allow-Credentials: true



```
GET / HTTP/1.1
Host: clients6.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: 1P_JAR=2018-11-12-03;
NID=144=boKA33UX4Ff3W6j5n47iywM62fKsrmjWAJYIJegtIAoqvgXXGA2fHUnmYTzT35JTE2TJVUBoL9g3FkPrfBkYx8q0c7ZBP-6e0846tdjH3q
xF2DAdrSsVF3z_OlBFDCP0kTLusA6z497XWiHoRtvPpIlQv0nn3M89x95KcvNMjeco0IHA_ETgfiPELzhaBWngbKZ4dodYyKP0C-TY2A;
OGP=-5061451:; SID=lwbXVvkaPSQolnU1TwaVAPxLJQ5aF1UOYFUhegSP4pzdTvNPDANnmsEE4VhzkKZmg_ln2w.;
HSID=AE458XdPJfmj54kBr; APISID=VCSDFd7eK_B_82k5/AEZxZfWEDtECNc1Pz; CONSENT=YES+IN.en+;
SIDCC=ABtHo-Fxd9nKesQv1lT9J9rzJoLcRSBF2FJdQvncCEVh8kxzXl0fgsOygJsx3H4I11l6QJH-1nE
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-Host: evilhosth3r0kU.com
Origin: http://evil.com
```



```
HTTP/1.1 404 Not Found
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Tue, 13 Nov 2018 06:19:46 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: http://evil.com
Vary: Origin
Vary: X-Origin
Content-Type: text/html; charset=UTF-8
Access-Control-Expose-Headers:
Cache-Control,Content-Encoding,Content-Length,Content-Type,Date,Expires,Pragma,Server,Vary,X-Google-GFE-Backend-R
equest-Cost
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 9
Server: GSE
Connection: close

Not Found
```

Host Header Injection

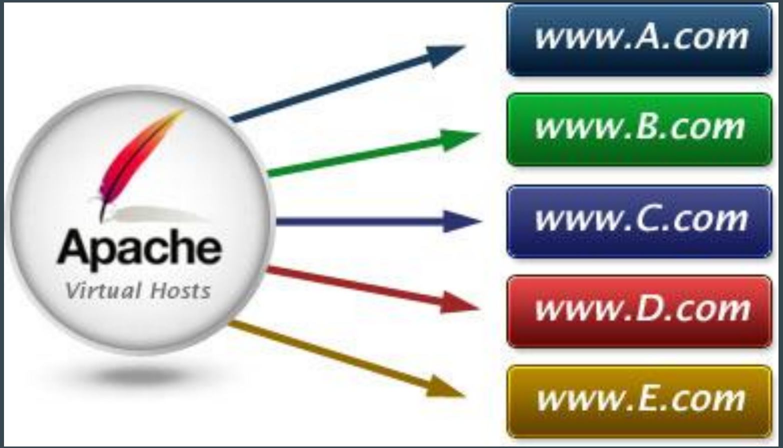
W - The host-Header tells the webserver which virtual host to use (if set up).

E - Causes redirection, Password Reset Poisoning(change host header to evil.com and reset link gets emailed as evil.com/token/lja830ru28f)

B - https://hackerone.com/reports/317476 ($7560)

D - Modify/Add X-Forwarded-Host header and

page redirects to evil.com

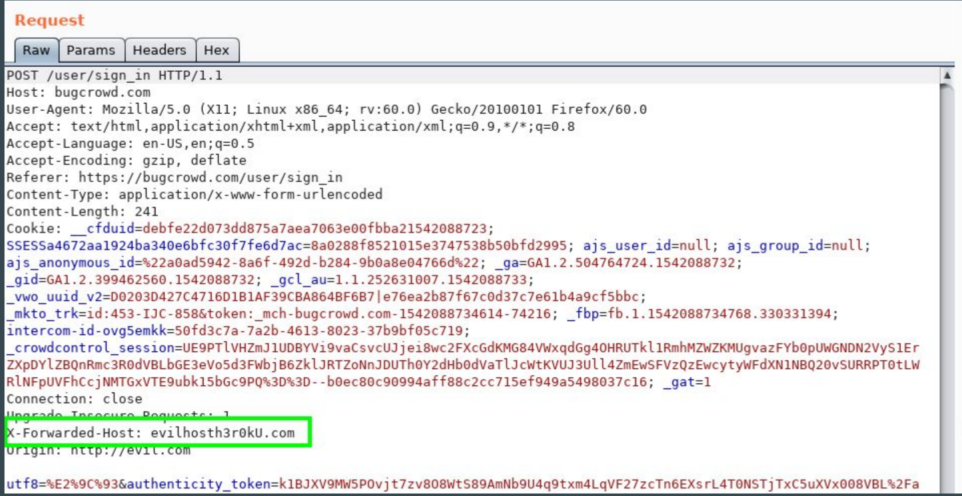


Host Header Injection (Cont..,)

Request headers - *X-Forwarded-Host: attacker.com*

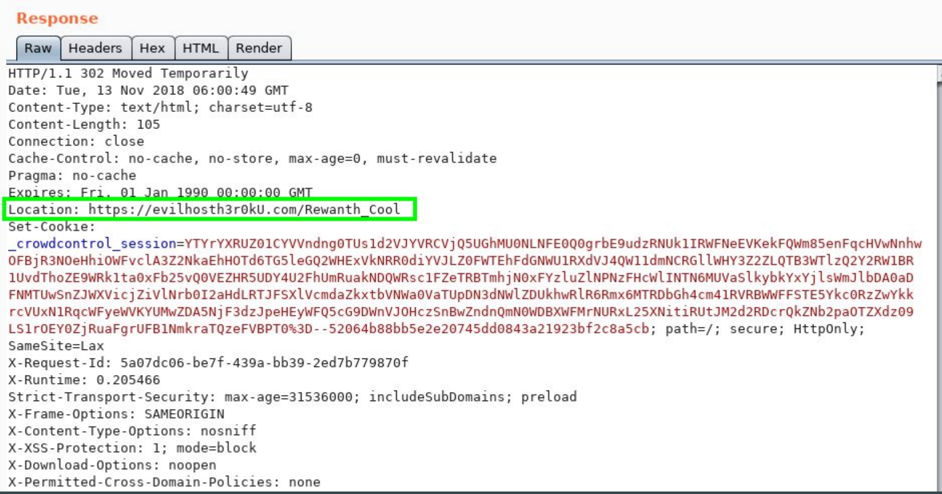
Response headers - Location: http://attacker.com/*

Find-virtual-hosts (https://pentest-tools.com/information-gathering/find-virtual-hosts)



```
POST /user/sign_in HTTP/1.1
Host: bugcrowd.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://bugcrowd.com/user/sign_in
Content-Type: application/x-www-form-urlencoded
Content-Length: 241
Cookie: __cfduid=debfe22d073dd875a7aea7063e00fbba21542088723;
SSESSa4672aa1924ba340e6bfc30f7fe6d7ac=8a0288f8521015e3747538b50bfd2995; ajs_user_id=null; ajs_group_id=null;
ajs_anonymous_id=%22a0ad5942-8a6f-492d-b284-9b0a8e04766d%22; _ga=GA1.2.504764724.1542088732;
_gid=GA1.2.399462560.1542088732; _gcl_au=1.1.252631007.1542088733;
_vwo_uuid_v2=D0203D427C4716D1B1AF39CBA864BF6B7|e76ea2b87f67c0d37c7e61b4a9cf5bbc;
_mkto_trk=id:453-IJC-858&token:_mch-bugcrowd.com-1542088734614-74216; _fbp=fb.1.1542088734768.330331394;
intercom-id-ovg5emkk=50fd3c7a-7a2b-4613-8023-37b9bf05c719;
_crowdcontrol_session=UE9PTlVHZmJ1UDBYVi9vaCsvcUJjei8wc2FXcGdKMG84VWxqdGg4OHRUTkl1RmhMZWZKMUgvazFYb0pUWGNDN2VyS1Er
ZXpDYlZBQnRmc3R0dVBLbGE3eVo5d3FWbjB6ZklJRTZoNnJDUTh0Y2dHb0dVaTlJcWtKVUJ3Ull4ZmEwSFVzQzEwcytyWFdXN1NBQ20vSURRPT0tLW
RlNFpUVFhCcjNMTGxVTE9ubk15bGc9PQ%3D%3D--b0ec80c90994aff88c2cc715ef949a5498037c16; _gat=1
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-Host: evilhosth3r0kU.com
Origin: http://evil.com

utf8=%E2%9C%93&authenticity_token=k1BJXV9MW5POvjt7zv8O8WtS89AmNb9U4q9txm4LqVF27zcTn6EXsrL4T0NSTjTxC5uXVx008VBL%2Fa
```



```
HTTP/1.1 302 Moved Temporarily
Date: Tue, 13 Nov 2018 06:00:49 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 105
Connection: close
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Location: https://evilhosth3r0kU.com/Rewanth_Cool
Set-Cookie:
_crowdcontrol_session=YTYrYXRUZ01CYVVndng0TUs1d2VJYVRCVjQ5UGhMU0NLNFE0Q0grbE9udzRNUk1IRWFNeEVKekFQWm85enFqcHVwNnhw
OFBjR3NOeHhiOWFvclA3Z2NkaEhHOTd6TG5leGQ2WHExVkNRR0diYVJLZ0FWTEhFdGNWU1RXdVJ4QW11dmNCRGllWHY3Z2ZLQTB3WTlzQ2Y2RW1BR
1UvdThoZE9WRk1ta0xFb25vQ0VEZHR5UDY4U2FhUmRuakNDQWRsc1FZeTRBTmhjN0xFYzluZlNPNzFHcWlINTN6MUVaSlkybkYxYjlsWmJlbDA0aD
FNMTUwSnZJWXVicjZiVlNrb0I2aHdLRTJFSXlVcmdaZkxtbVNWa0VaTUpDN3dNWlZDUkhwRlR6Rmx6MTRDbGh4cm41RVRBWWFFSTE5Ykc0RzZwYkk
rcVUxN1RqcWFyeWVKYUMwZDA5NjF3dzJpeHEyWFQ5cG9DWnVJOHczSnBwZndnQmN0WDBXWFMrNURxL25XNitiRUtJM2d2RDcrQkZNb2paOTZXdz09
LS1rOEY0ZjRuaFgrUFB1NmkraTQzeFVBPT0%3D--52064b88bb5e2e20745dd0843a21923bf2c8a5cb; path=/; secure; HttpOnly;
SameSite=Lax
X-Request-Id: 5a07dc06-be7f-439a-bb39-2ed7b779870f
X-Runtime: 0.205466
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
```

Clickjacking

W - Used to load/embed particular iframes in a website

E - Attackers can load embedded hidden iframes if options are not set properly.

B - https://medium.com/@raushanraj_65039/google-clickjacking-6a04132b918a ($12600)

D - if x-frame-options is missing, then its likely vulnerable to clickjacking

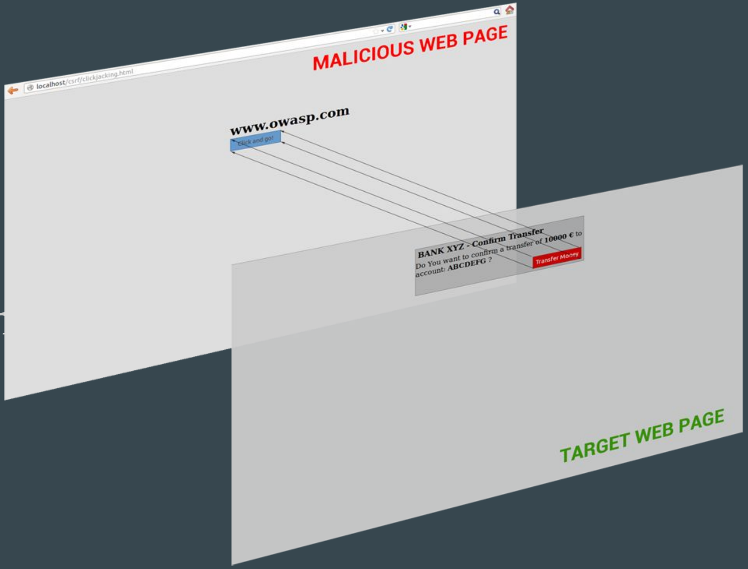
Clickjacking (Cont..,)

Response headers -

X-Frame-Options: DENY

X-Frame-Options: SAMEORIGIN

X-Frame-Options: ALLOW-FROM *.domain.com

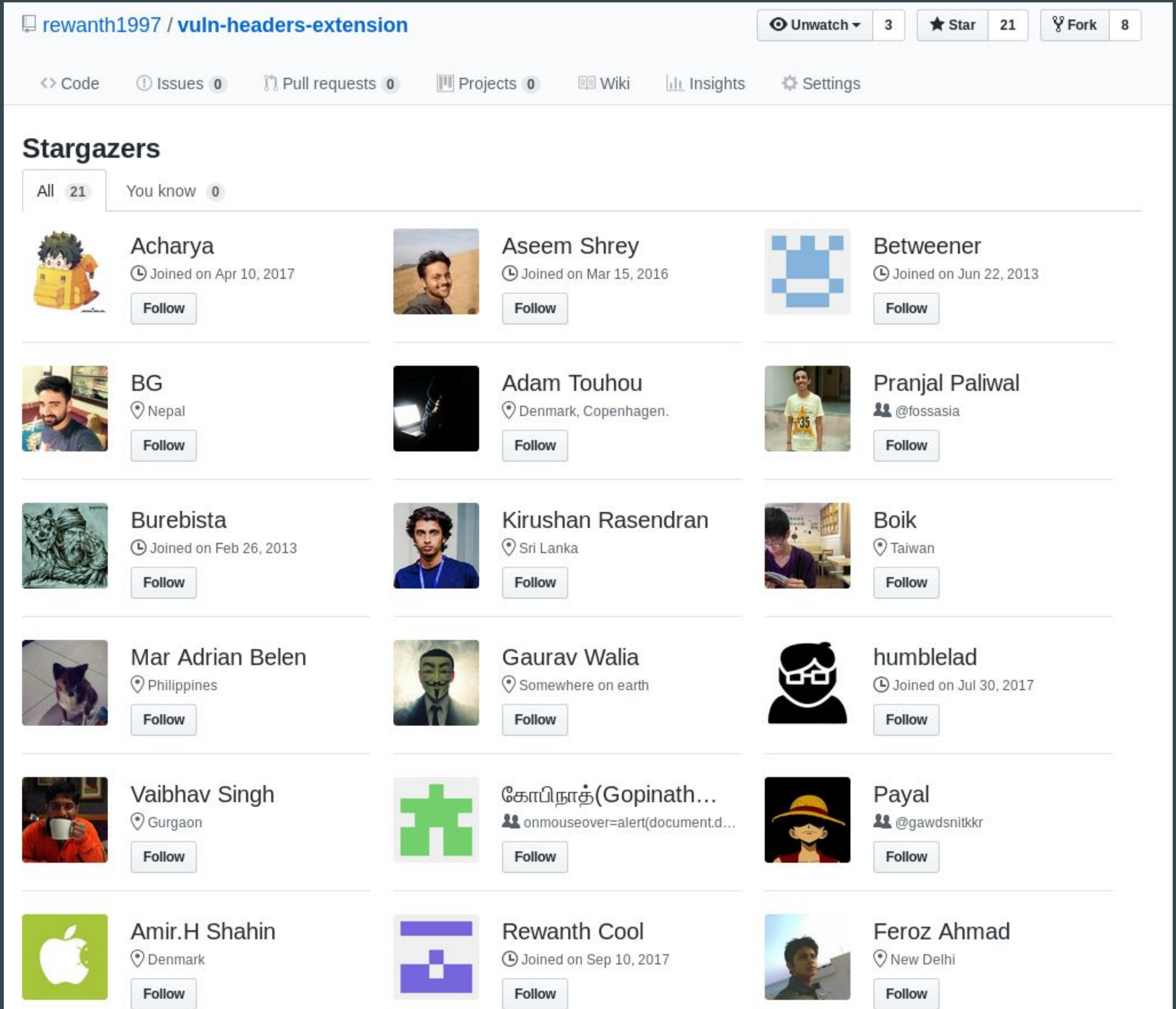


Do You want to confirm a transfer of **10000 €** to account: **ABCDEFG** ?

vuln-headers-extension

https://github.com/rewanth1997/vuln-headers-extension/

https://medium.com/@rewanthcool/firefox-vuln-headers-extension-e848b6d80d14



rewanth1997 / **vuln-headers-extension**

Stargazers

All 21 | You know 0

Acharya	Joined on Apr 10, 2017
Aseem Shrey	Joined on Mar 15, 2016
Betweener	Joined on Jun 22, 2013
BG	Nepal
Adam Touhou	Denmark, Copenhagen.
Pranjal Paliwal	@fossasia
Burebista	Joined on Feb 26, 2013
Kirushan Rasendran	Sri Lanka
Boik	Taiwan
Mar Adrian Belen	Philippines
Gaurav Walia	Somewhere on earth
humblelad	Joined on Jul 30, 2017
Vaibhav Singh	Gurgaon
கோபிநாத்(Gopinath…	onmouseover=alert(document.d…
Payal	@gawdsnitkkr
Amir.H Shahin	Denmark
Rewanth Cool	Joined on Sep 10, 2017
Feroz Ahmad	New Delhi

Creating firefox extension

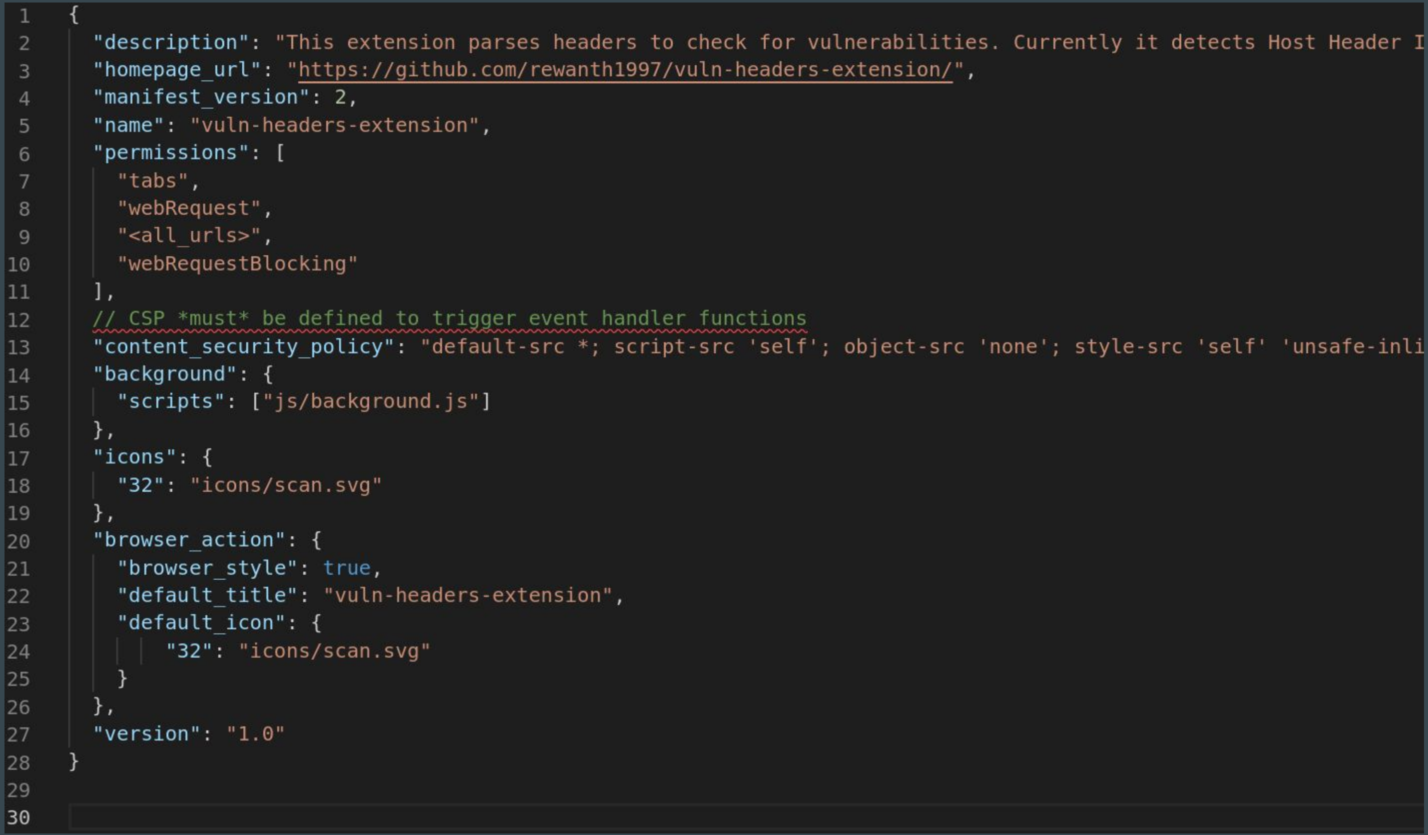
manifest.json

browser.browserAction.onClicked.addListener()

browser.webRequest.onBeforeSendHeaders.addListener(...)

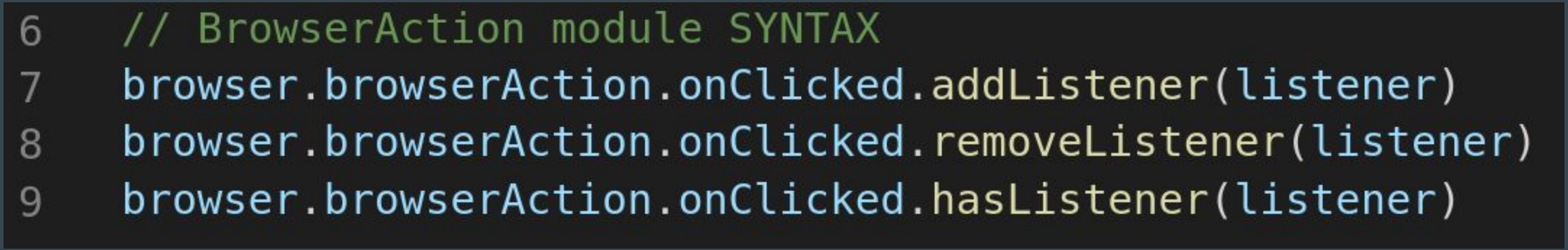
browser.webRequest.onHeadersReceived.addListener(...)

manifest.json



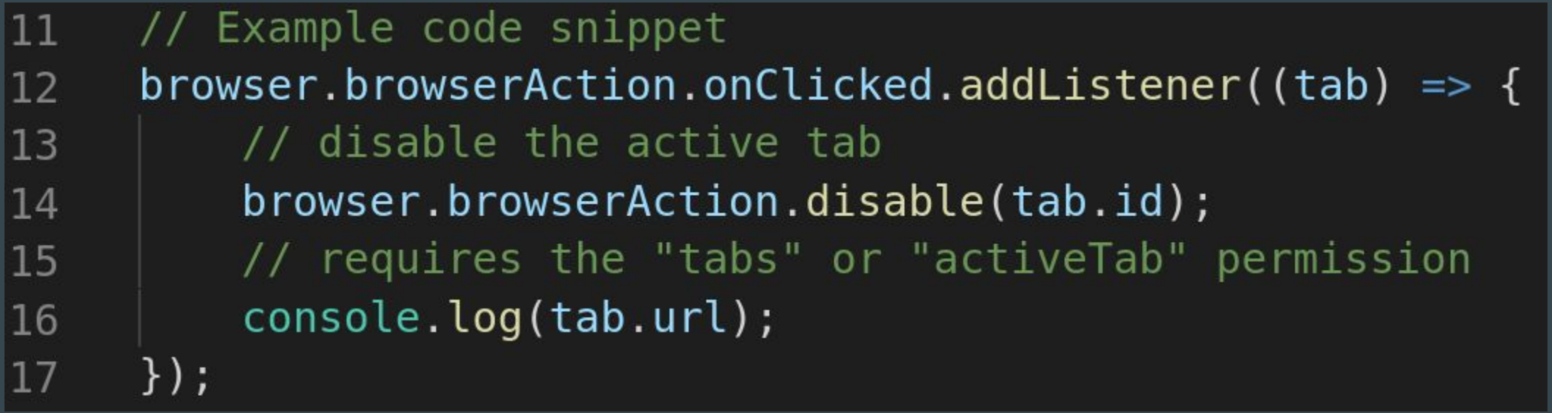
```
{
  "description": "This extension parses headers to check for vulnerabilities. Currently it detects Host Header I
  "homepage_url": "https://github.com/rewanth1997/vuln-headers-extension/",
  "manifest_version": 2,
  "name": "vuln-headers-extension",
  "permissions": [
    "tabs",
    "webRequest",
    "<all_urls>",
    "webRequestBlocking"
  ],
  // CSP *must* be defined to trigger event handler functions
  "content_security_policy": "default-src *; script-src 'self'; object-src 'none'; style-src 'self' 'unsafe-inli
  "background": {
    "scripts": ["js/background.js"]
  },
  "icons": {
    "32": "icons/scan.svg"
  },
  "browser_action": {
    "browser_style": true,
    "default_title": "vuln-headers-extension",
    "default_icon": {
      "32": "icons/scan.svg"
    }
  },
  "version": "1.0"
}
```

browserAction event listeners



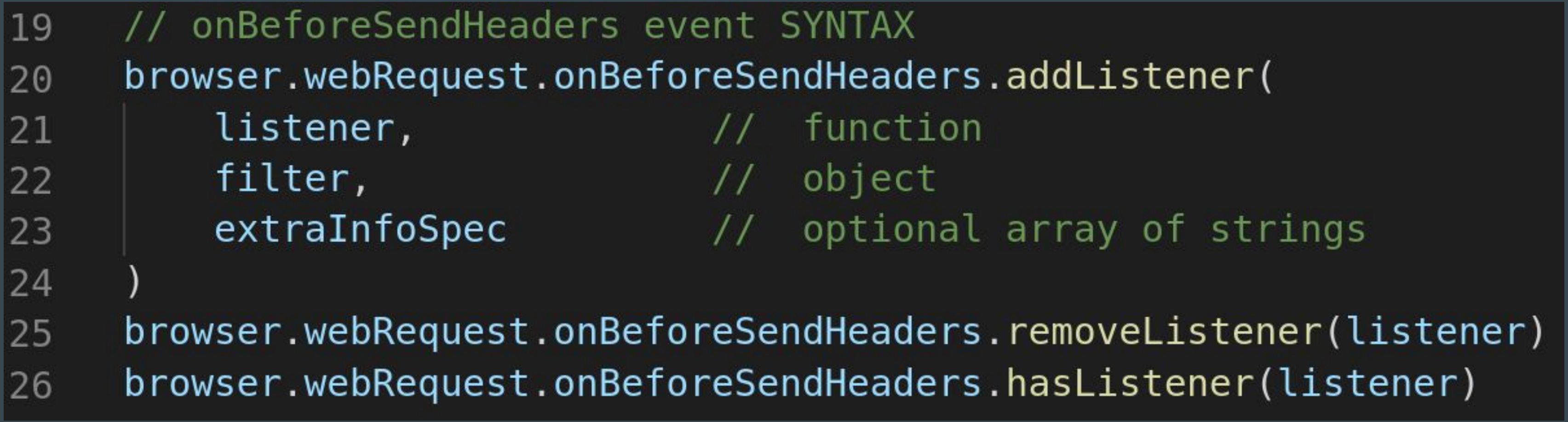
```
// BrowserAction module SYNTAX
browser.browserAction.onClicked.addListener(listener)
browser.browserAction.onClicked.removeListener(listener)
browser.browserAction.onClicked.hasListener(listener)
```

browserAction event SYNTAX



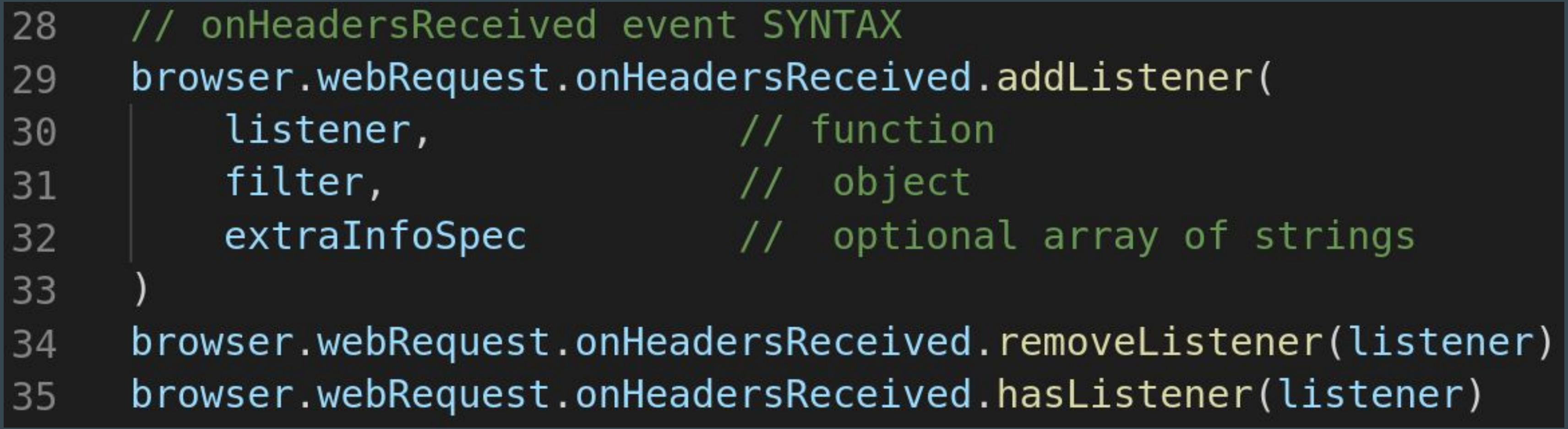
```
// Example code snippet
browser.browserAction.onClicked.addListener((tab) => {
    // disable the active tab
    browser.browserAction.disable(tab.id);
    // requires the "tabs" or "activeTab" permission
    console.log(tab.url);
});
```

onBeforeSendHeaders event SYNTAX



```
// onBeforeSendHeaders event SYNTAX
browser.webRequest.onBeforeSendHeaders.addListener(
    listener,             //  function
    filter,               //  object
    extraInfoSpec         //  optional array of strings
)
browser.webRequest.onBeforeSendHeaders.removeListener(listener)
browser.webRequest.onBeforeSendHeaders.hasListener(listener)
```

onHeadersReceived event SYNTAX



```
// onHeadersReceived event SYNTAX
browser.webRequest.onHeadersReceived.addListener(
    listener,             // function
    filter,               //  object
    extraInfoSpec         //  optional array of strings
)
browser.webRequest.onHeadersReceived.removeListener(listener)
browser.webRequest.onHeadersReceived.hasListener(listener)
```

DEMO TIME

Any doubts?

THANK YOU