



Web Application Security Testing Using Burp Suite

Rupesh Garg & Chandra Sekhar Gajula



Agenda



Introduction



Approach



Challenges Faced



Benefits



Conclusion

What does Security Breach Means?



- An act from outside an organization that bypasses or contravenes security policies, practices, or procedures. A similar internal act is called security violation.

3 biggest security breaches of Recent times.

- 1) Heartland Payment Systems- In Mar 2008 – 138 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.
- 2) TJX Companies Inc. – In Dec 2006- 94 million credit cards exposed
- 3) Epsilon- In Mar 2011- Exposed names and e-mails of millions of customers stored in more than 108 retail stores plus several huge financial firms like CitiGroup Inc. and the non-profit educational organization, College Board.



Introduction

- This document will detail how you can use the Burp Suite to test web applications for common vulnerabilities like Cross Site Scripting, SQL Injection. It gives brief details about each component and its uses.
- Web Application Security Testing is an in-depth assessment of the application web pages to identify inherent and potential vulnerabilities. It determines the confidentiality, integrity and availability of the application.
- Web security testing is using a variety of tools, both manual and automatic, to simulate and stimulate the activities of our web application. We will get malicious inputs like cross-site scripting attacks and use both manual and scripted methods to submit them to our web application. We will use malicious SQL inputs in the same way, and submit them also.
- It is our goal to produce repeatable, consistent tests that fit into our overall testing scheme, but that address the security side of web applications. When someone asks whether our application has been tested for security, we will be able to confidently say yes and point to specific test results to back up our claim.



Web Application Security Testing

- “ Web Application Security Testing tells about how you can test for SQL injection or cross-site scripting, but it won’t provide a comprehensive set of malicious inputs that you can use”

Below Figure shows many points within a system that might require protection

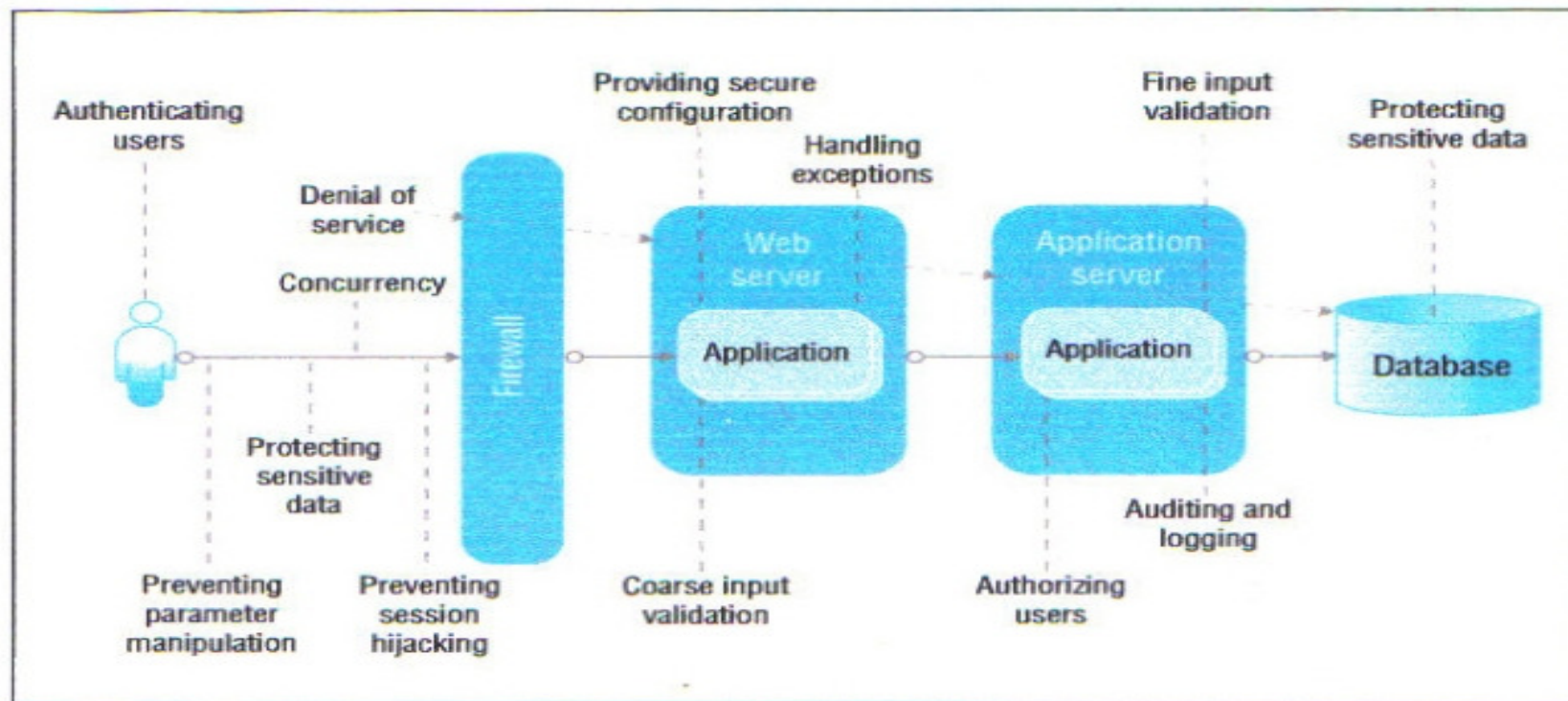


Figure 1: Web application security concerns



OWASP Top 10 Web Application Security Risks (2010)

- The OWASP Top Ten provides a powerful awareness document for web application security.
- The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

A1: Injection

A2: Cross-Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross-Site Request Forgery (CSRF)

A6: Security Misconfiguration

A7: Insecure Cryptographic Storage

A8: Failure to Restrict URL Access

A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards



About Burp Suite:

- Burp professional Suite is an integrated platform for Security Testing of web applications. It includes the entire set of Burp tools with numerous interfaces, designed to assist and accelerate the process of security testing.

Key features unique to Burp Suite include:

- ❖ Detailed analysis and rendering of requests and responses.
- ❖ One-click transfer of interesting requests between tools.
- ❖ Utilities for decoding and comparing application data.
- ❖ Support for custom client and server SSL certificates.
- ❖ Burp Scanner to automate findings of vulnerabilities
- ❖ Centrally configured settings for downstream proxies, web and proxy authentication, and logging.
- ❖ Tools can run in a single tabbed window, or be detached in individual windows.



Approach

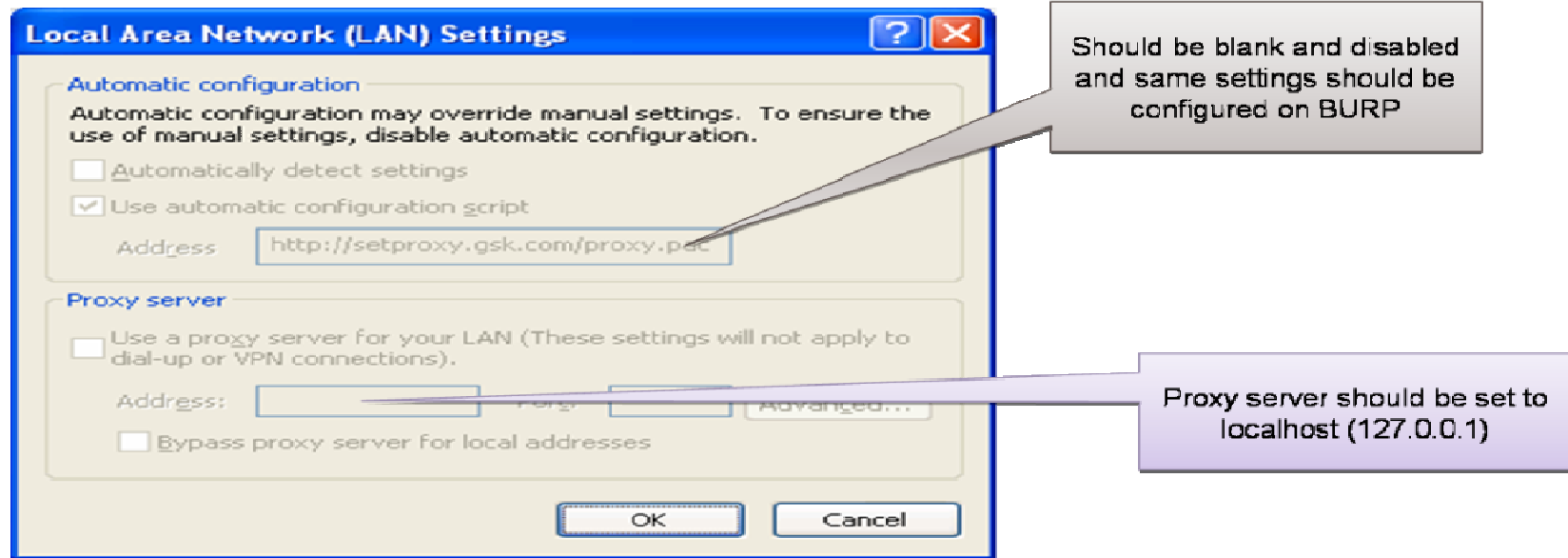


How to configure BURP and BROWSER?

- ❖ Burp Proxy allows defining multiple listeners. Each listener opens a port on the computer and waits for connections from the browser. By default, Burp opens a single listener on port 8080 of the loop back interface. For each listener, the following properties need to be configured as applicable.
- **Local listener port** - This is the port on the local computer which will be opened to listen for incoming connections. Browser settings should be configured to use the host 127.0.0.1 and the Port 8080 as its proxy server.
- **Use of proxy server** - This controls whether Burp Suite communicates directly with remote web servers, or via a downstream HTTP proxy (located at the server and port number specified). Many LAN configurations require users to access web servers via a central proxy. Burp Suite can be used in this type of set-up by configuring the address and port number of the proxy server here; GSK Internet proxy in this case.

How to configure BURP and BROWSER? Contd..

- By doing below browser configuration, you are making your browser to interact with BURP not with the server.



- BURP needs to be configured now so that it can accept the request from browser and from there on it can become a browser for the server

BURP Configuration

- Click on options tab and just consider the three sections, rest all sections be as it is with there default settings
 - Do www authentication (used for intranet application)
 - Upstream proxy server (used for internet application)
 - Use client SSL certificate (PKCS12)

Intranet Application Settings:

- ❖ **Method 1:** Check the do www authentication check box and add the server details where application is hosted, type of authentication (basic, NTLM or digest. This can be directly asked to development team or hit and trial can be done as there are only three options available), username, password and domain
- ❖ **Method 2:** Check the do www authentication check box and check the prompt for credentials on authentication failure checkbox too, by doing so no need to enter the above details, these details can be entered while you start running the application via burp

➤ **Internet Application Settings:** In upstream proxy server section, enter the details like destination host (not mandatory), proxy host (e.g. Wipro Proxyxxx.xx.xxx.x, Client Proxy is xxxxx.xxx.com or xxxxx.xxxx.com), proxy port (e.g. 800 for Client and Wipro), Authentication (hit and trial incase of no information on this as there are only three options available), Username, Password, Domain and hostname (not mandatory). Once these details are filled click on add button. All details shall be moved to the above table of upstream proxy server.

Key Components of Burp Suite

➤ Burp Suite has 2 editions:

- ❖ **BURP Suite Free Edition:** Burp Proxy, Burp Spider, Burp Repeater, Burp Sequencer, Burp Decoder, Burp Comparer, Burp Intruder (Time-throttled demo version)
- ❖ **BURP Suite Professional:** It has all components including Burp Scanner and Burp Intruder (Full edition, lightening fast ability to save and restore attacks, built-in attack payloads)

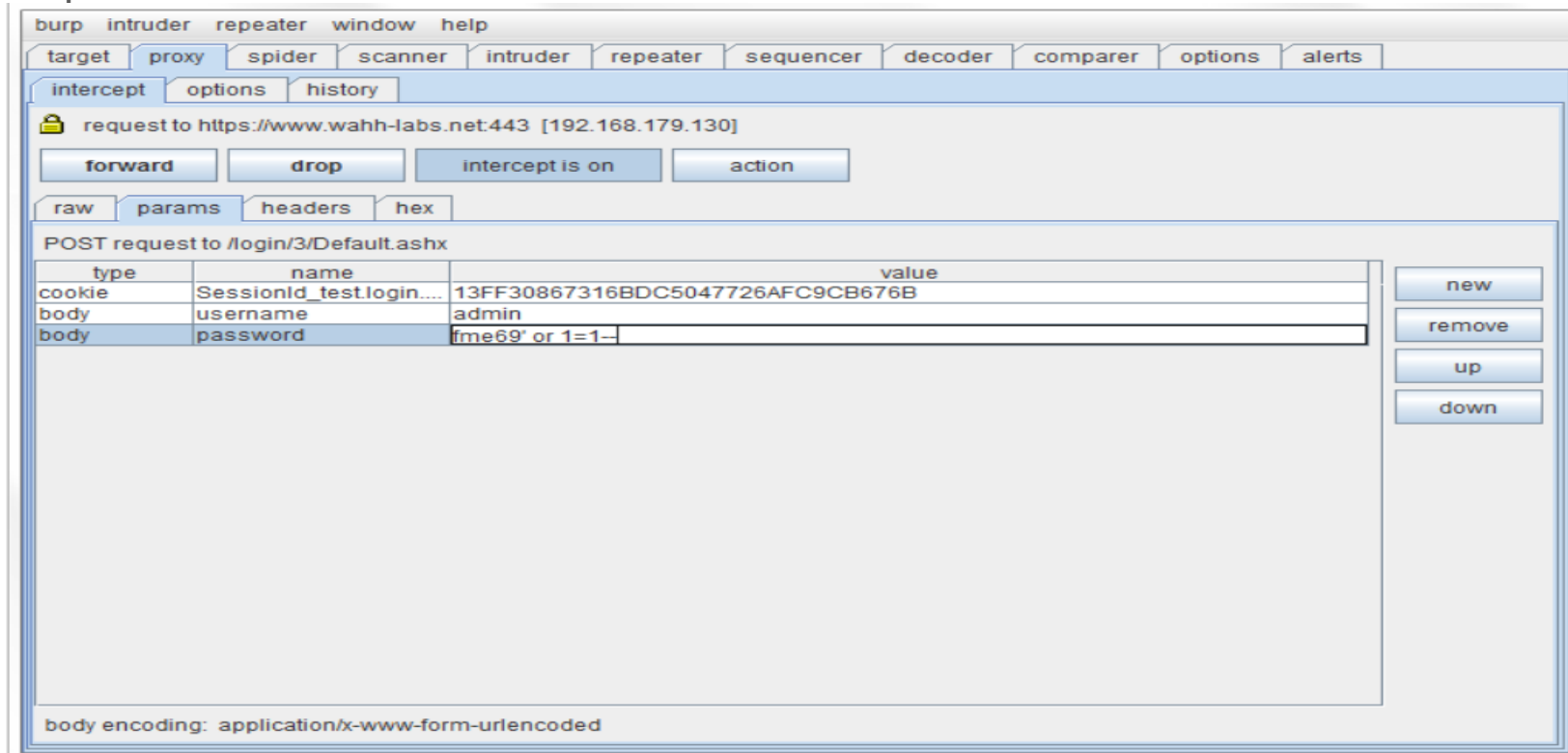
➤ Burp Proxy:

When Burp has been configured to become a browser's proxy, it will capture and replay any and all web requests. By default, Burp will intercept the web request and wait for approval/modification before passing it on to the internet. This type of control can allow a person to dynamically change variables to see what happens.



Burp Proxy- Intercept Tab

- This tab is used to display and modify individual browser requests and server responses.
- If “*intercept is on*” is switched off then no request will be intercepted by burp proxy. So the tester can on the interceptor only for those requests where any vulnerability can be sensed, instead of intercepting each and every request.



Burp Proxy- OptionsTab

- This tab contains various configuration options which control the behavior of Burp Proxy, as described below

proxy listeners

running	port	loopback only	support invisible	redirect	cert
<input checked="" type="checkbox"/>	8080	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

To add a new listener, complete the relevant details and click "add".

local listener port:

☐ listen on loopback interface only

☐ support invisible proxying for non-proxy-aware clients

redirect to host:

redirect to port:

☐ use a custom server SSL certificate (PKCS12)

file

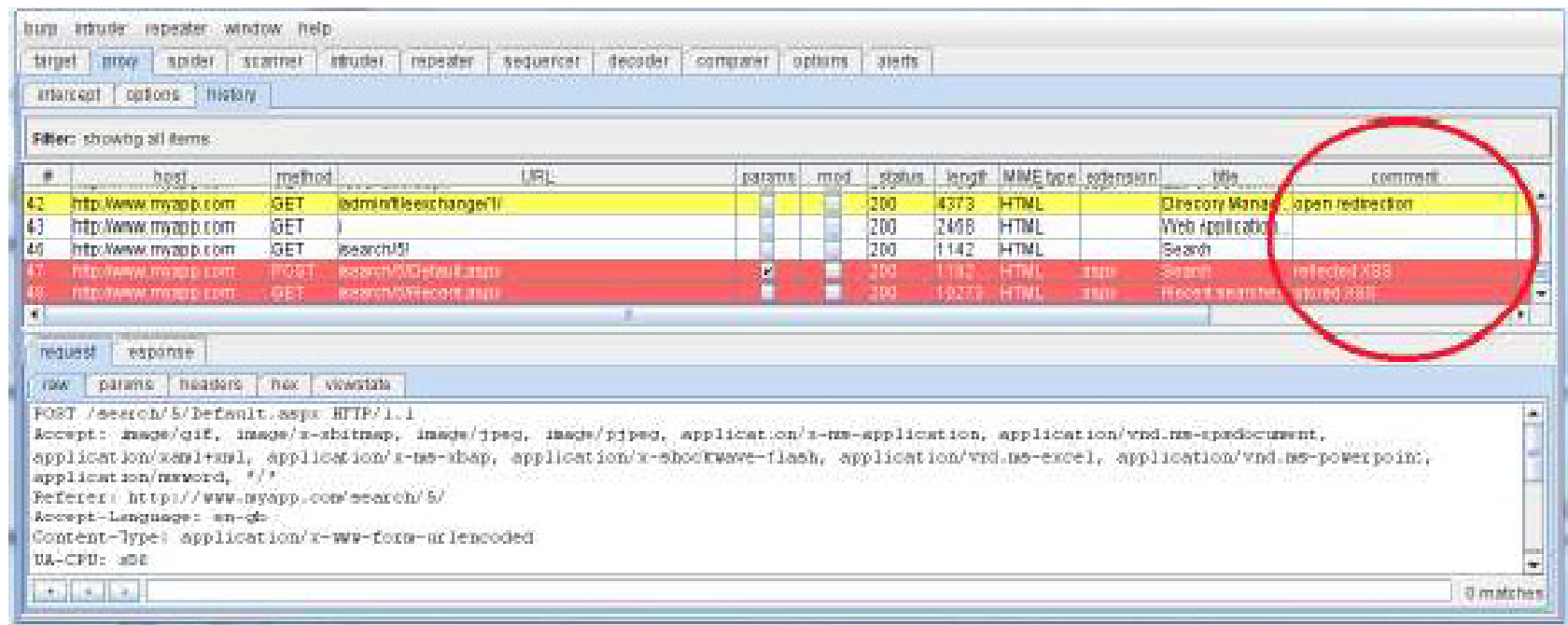
password

- Burp Proxy allows you to define multiple listeners. Each listener opens a port on your computer and waits for connections from your browser. By default, Burp opens a single listener on port 8080 of the loopback interface, but you can modify this listener and add as many others as you require



Burp Proxy- HistoryTab

- This tab displays details of all requests made, and shows the target server and portnumber, the HTTP method, the URL, whether the request contains parameters or was manually modified, the HTTP status code of the response, the response size in bytes, the MIME type of the response, the file type of the requested resource, the title of the HTML page, whether SSL was used, the remote IP address, any cookies set by the server, and the time of the request.



Burp Proxy Uses:

- ✓ Intercept and modify all HTTP/S traffic passing in both directions.
- ✓ Send interesting items to other Burp Suite tools with a single click
- ✓ View all traffic in the detailed proxy history, with advanced filters and search functions.



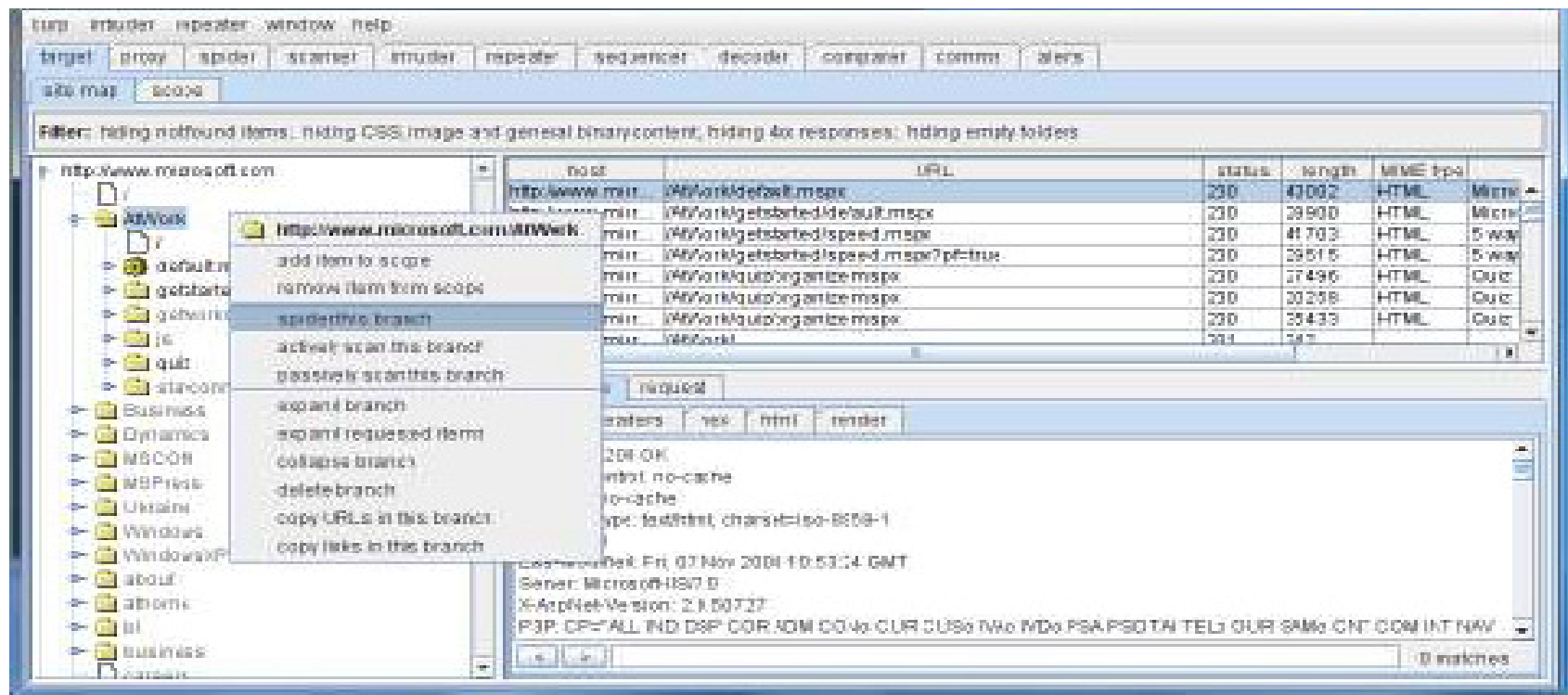
Burp Spider

- Burp Spider is a tool for mapping web applications. It uses various intelligent techniques to generate a comprehensive inventory of an application's content and functionality.
- Burp Spider maps a target application by following hyperlinks found within HTML and JavaScript, submitting forms, and using other clues such as directory listings, source code comments and the robots.txt file. Results are displayed in the target site map in both tree and table format, providing a clear and highly detailed view of the target application.
- Burp Spider enables you to obtain a detailed understanding of how a web application works, avoiding the time-consuming and unreliable task of manually following links, submitting forms and scouring HTML source code. Potentially vulnerable application functions can be quickly identified, allowing you to check for specific vulnerabilities such as “*SQL injection and directory traversal*”.



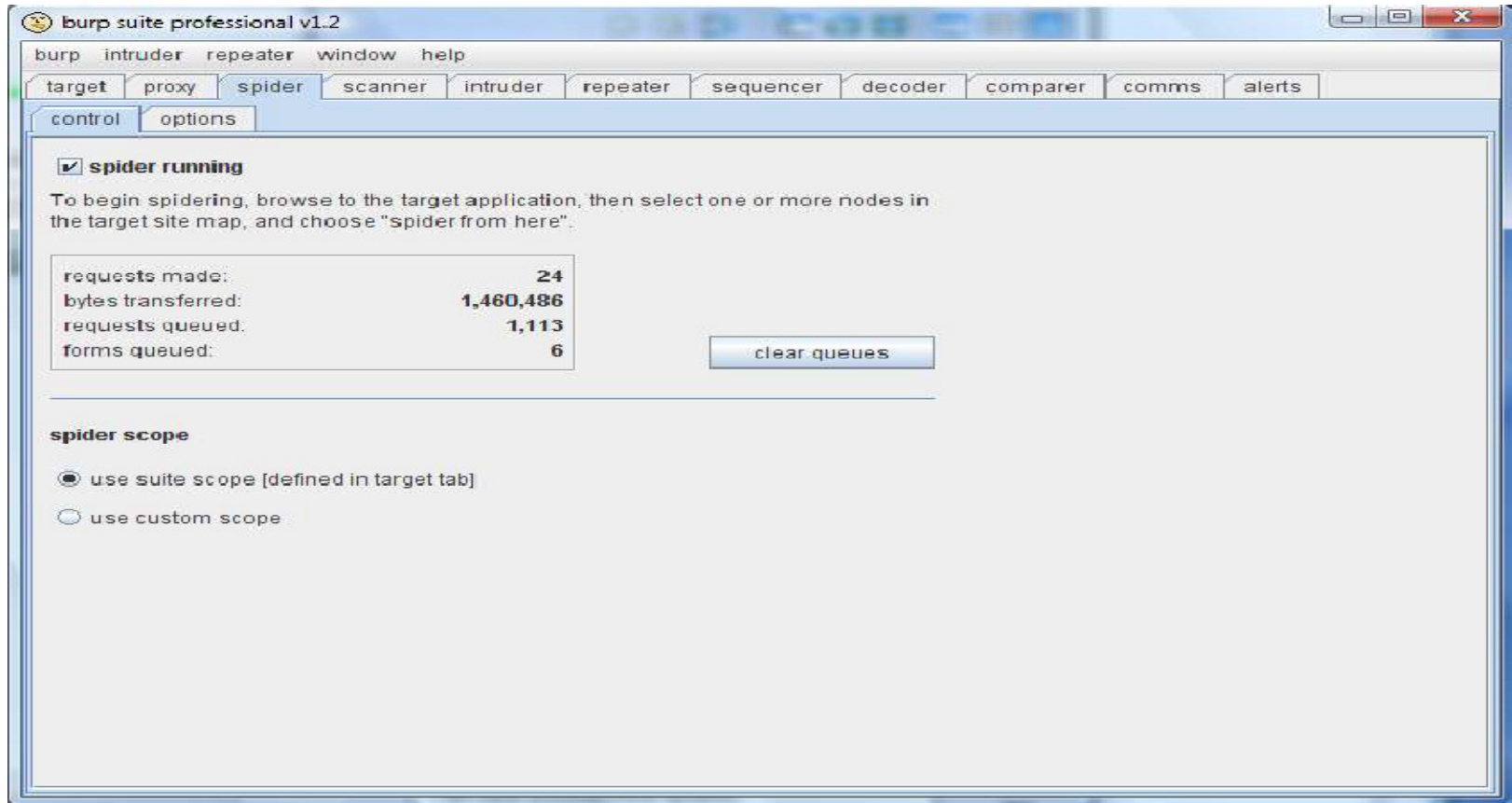
Using Burp Spider

- To use Burp Spider against an application requires two simple steps:
 - ❖ With your browser configured to use Burp Proxy as its proxy server, browse to the target application. (You can turn off interception within the Proxy, to savetime.)
 - ❖ Go to the site map in the "target" tab, and select the host(s) and directories where the target application resides. Choose the "spider this host/branch" option from the context menu.



Burp Spider- Control Tab

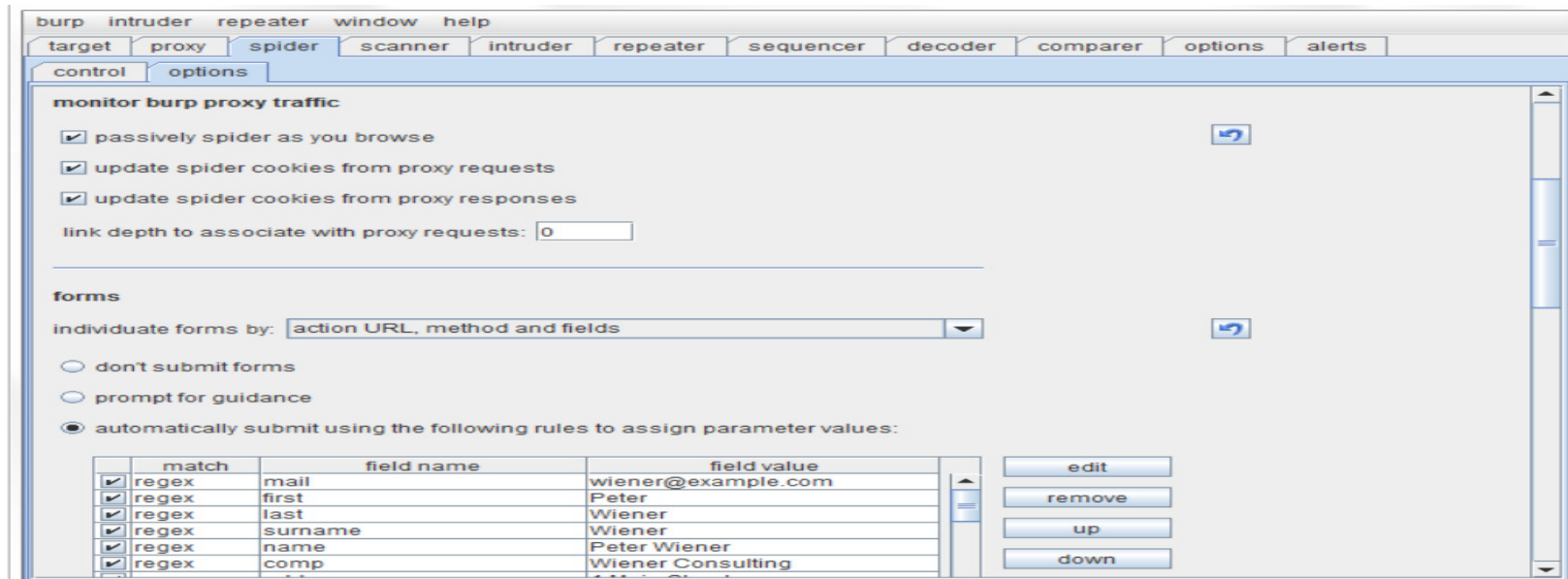
- This tab is used to start and stop Burp Spider, monitor its progress, and define the spidering scope



Burp Spider- OptionsTab

- This tab contains various configuration options which control the behaviour of BurpSpider, as described below. These settings can be modified after the Spider has started running, and will be applied retrospectively to prior results.

For example, if the maximum link depth is increased, then links which were previously outside the maximum depth will be queued to be requested if appropriate.



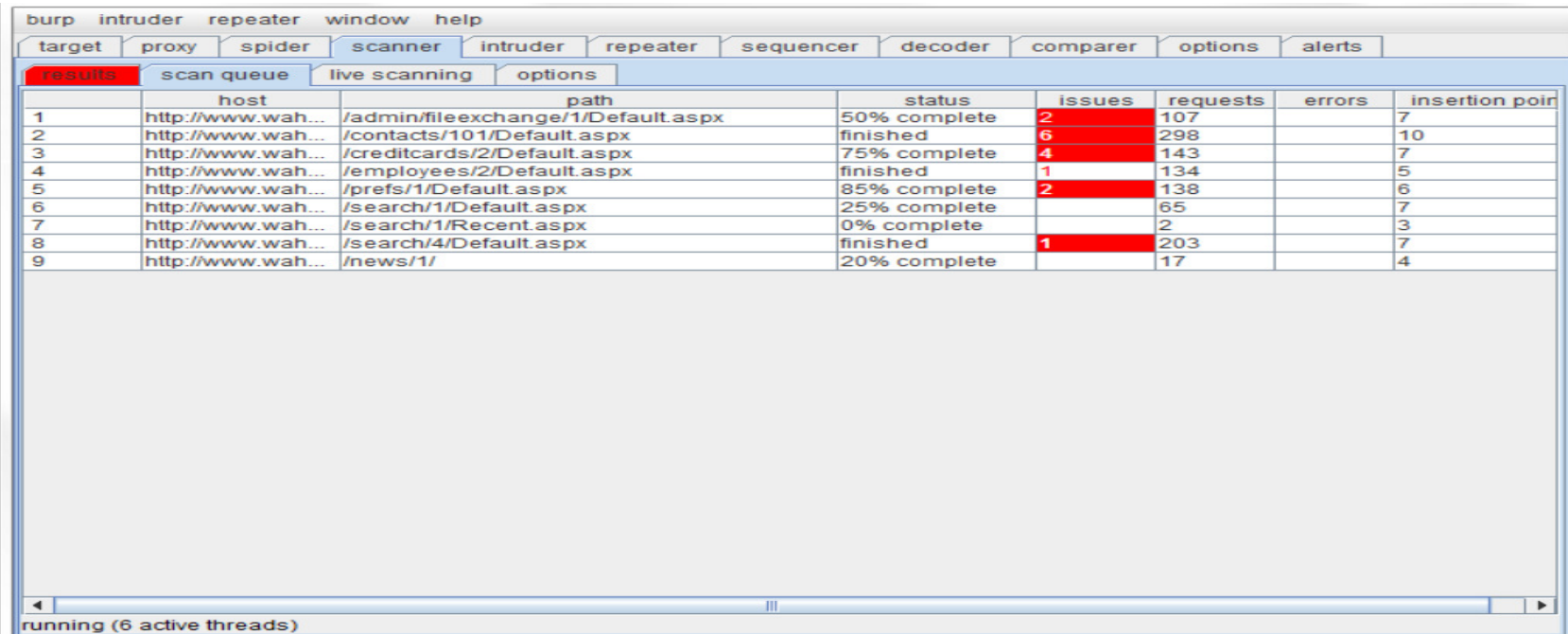
Burp Spider Uses:

- Spider deal with complex applications, with automatic handling of login credentials and session cookies, and detection of custom "not found" responses.



Burp Scanner

- Burp Scanner is a tool for performing automated discovery of security vulnerabilities in web applications. It is designed to be used by penetration testers, and to fit in closely with your existing techniques and methodologies for performing manual and semi-automated penetration tests of web applications.



The screenshot shows the Burp Scanner interface with the 'results' tab selected. The table displays the following data:

	host	path	status	issues	requests	errors	insertion point
1	http://www.wah...	/admin/fileexchange/1/Default.aspx	50% complete	2	107		7
2	http://www.wah...	/contacts/101/Default.aspx	finished	6	298		10
3	http://www.wah...	/creditcards/2/Default.aspx	75% complete	4	143		7
4	http://www.wah...	/employees/2/Default.aspx	finished	1	134		5
5	http://www.wah...	/prefs/1/Default.aspx	85% complete	2	138		6
6	http://www.wah...	/search/1/Default.aspx	25% complete		65		7
7	http://www.wah...	/search/1/Recent.aspx	0% complete		2		3
8	http://www.wah...	/search/4/Default.aspx	finished	1	203		7
9	http://www.wah...	/news/1/	20% complete		17		4

running (6 active threads)



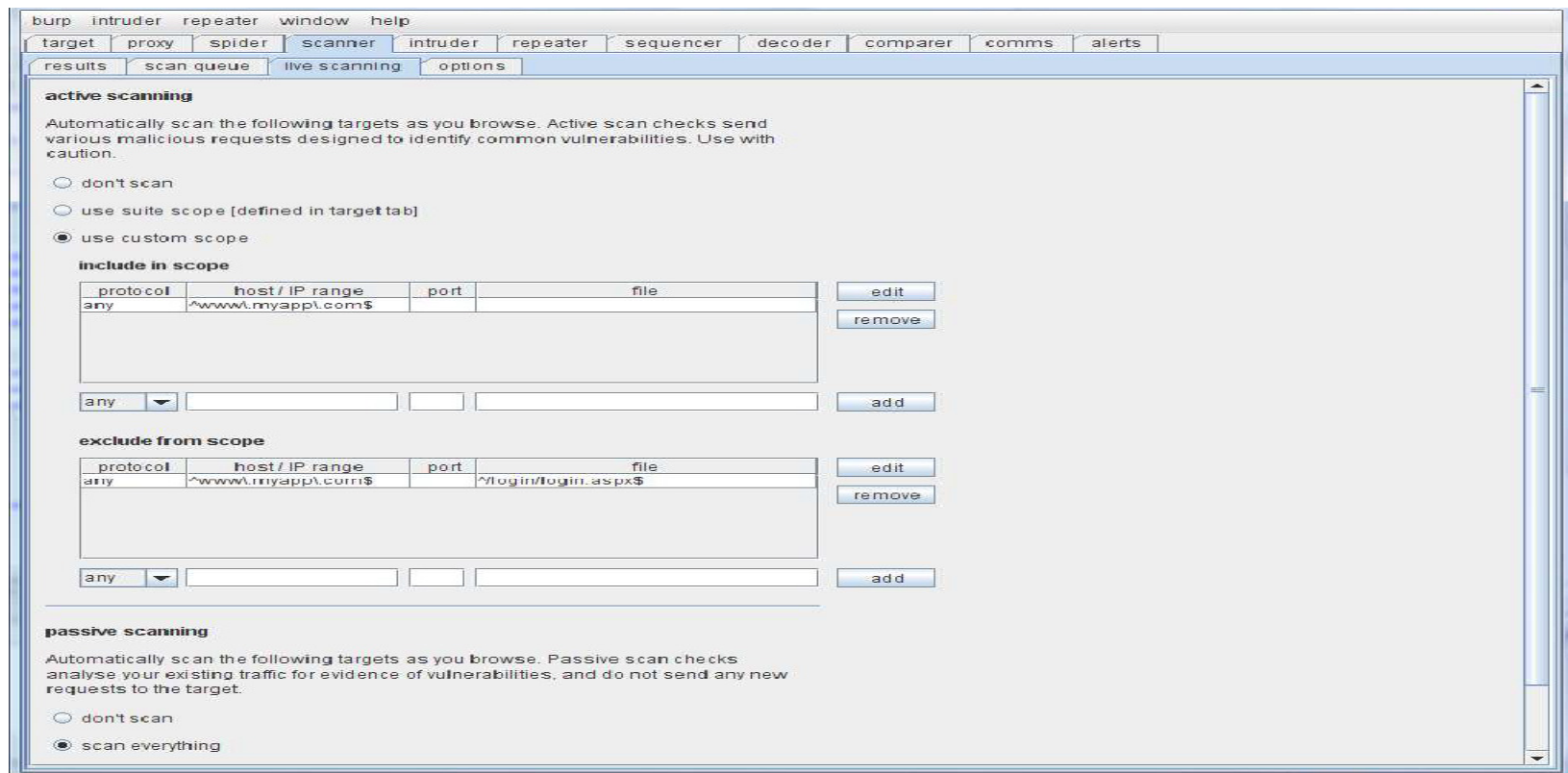
Burp Scanner – View the Identified Issue

- You can double-click any item in the scan queue to display the issues identified so far, and view the base request and response for that item



Burp Scanner- Live Scanning Tab

- A further way to initiate scans is to use the "live scanning" feature. In this mode, you tell Burp what your target scope is for active and passive scanning, and it will automatically initiate active or passive scans against relevant requests as you use the application.



Burp Scanning Uses:

- **Active scanning** : The scanner sends various crafted requests to the application, derived from a base request, and analyses the resulting responses looking for vulnerable behaviour.
- The issues that Burp's active scanning is able to identify mostly fall into two categories:
 - ❖ Input-based vulnerabilities targeting the client side, such as cross-site scripting, HTTP header injection, and open redirection.
 - ❖ Input-based vulnerabilities targeting the server side, such as SQL injection, OS command injection, and file path traversal.

Burp Scanning Uses Contd..

➤ **Passive Scanning:** The scanner doesn't send any new requests of its own; it merely analyses the contents of existing requests and responses, and deduces vulnerabilities from those. Burp Scanner is able to identify numerous kind of vulnerabilities using solely passive techniques, including

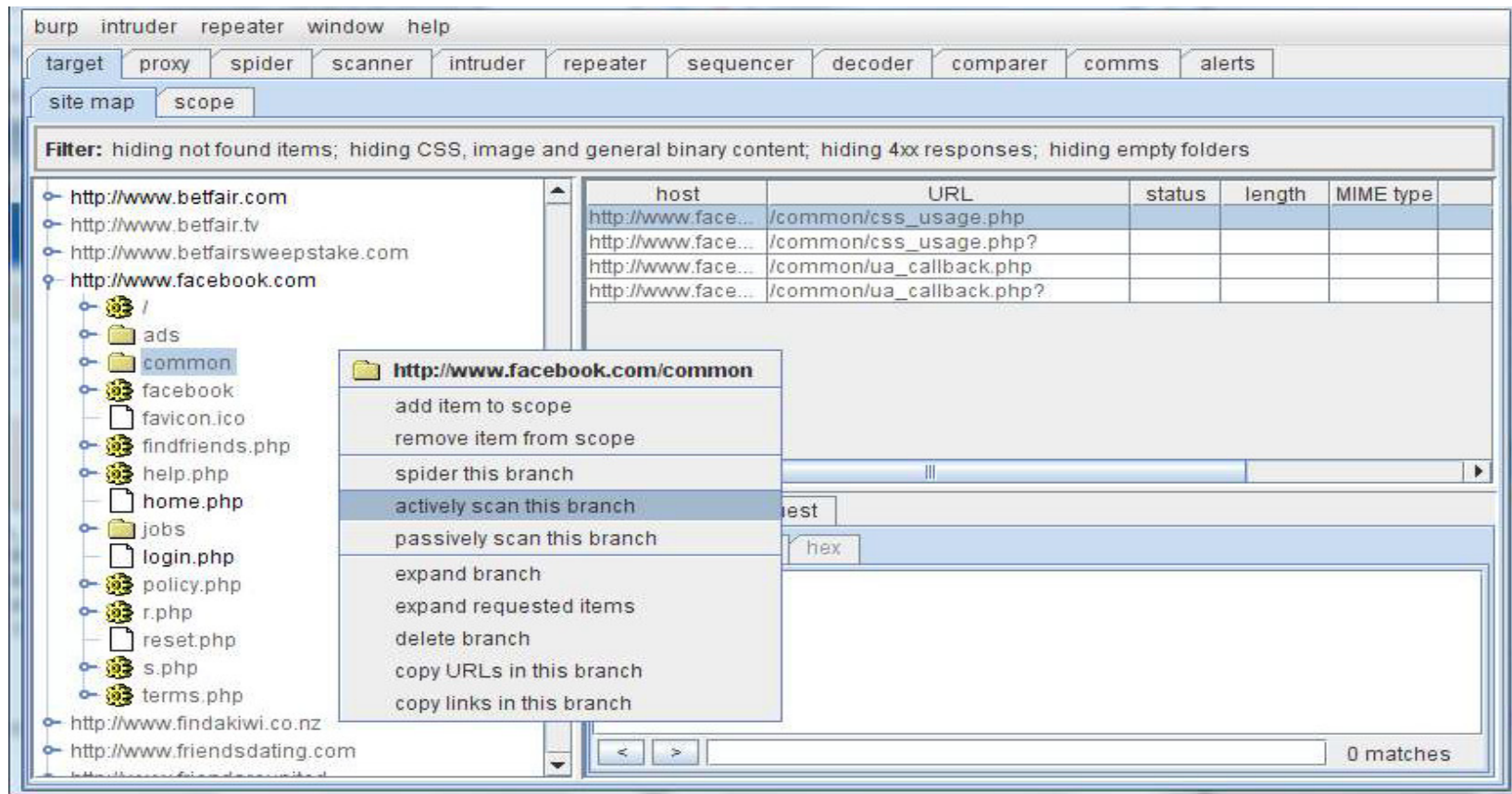
- Clear-text submission of passwords.
- Insecure cookie attributes, like missing HttpOnly and secure flags.
- Liberal cookie scope.
- Cross-domain script includes and Referer leakage.
- Forms with autocomplete enabled.
- Caching of SSL-protected content.
- Directory listings.
- Submitted passwords returned in later responses.
- Insecure transmission of session tokens.
- Leakage of information like internal IP addresses, email addresses, stack traces, etc
- Insecure ViewState configuration.
- Ambiguous, incomplete, incorrect or non-standard Content-type directives



Burp Scanning Uses Contd..

Burp Scanner- User- directed scanning

- This lets you select specific requests within any of the Burp Suite tools, and send these for active or passive scanning

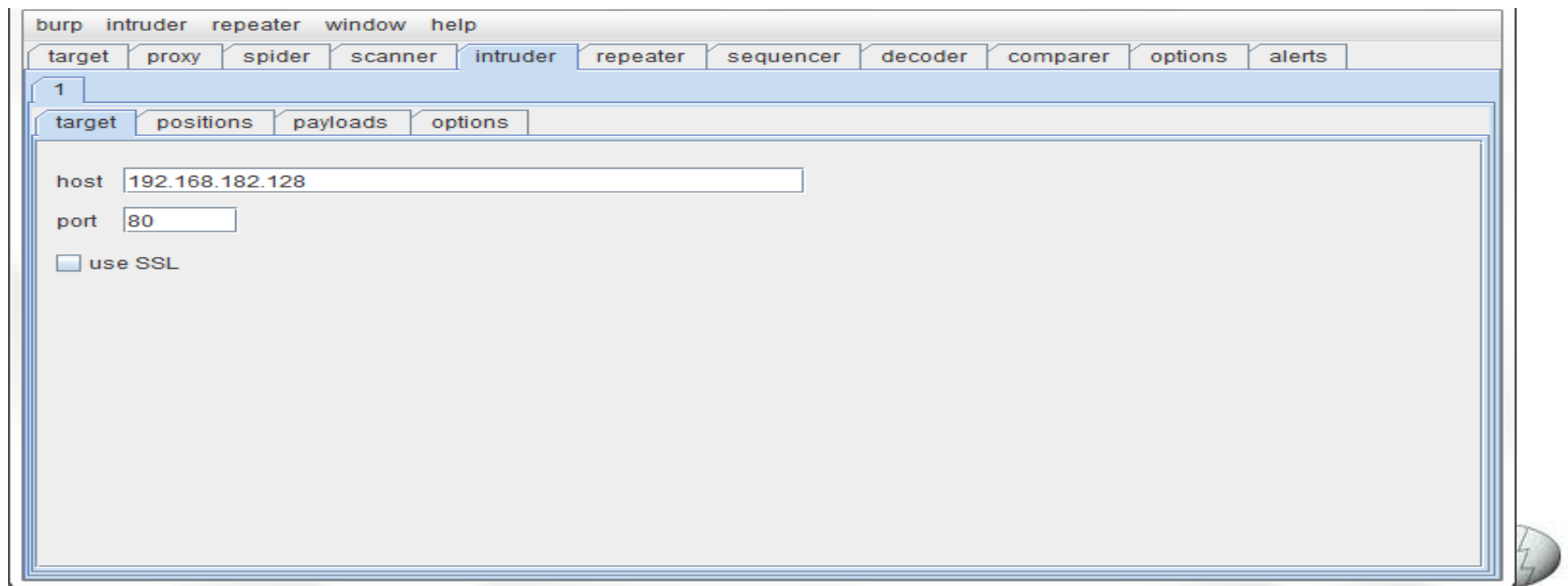


Burp Intruder

- Burp Intruder is a tool for automating customised attacks against web applications.
- Burp Intruder is not a point-and-click tool. To use it effectively you need to understand how the target application functions, and have some knowledge of the HTTP protocol.

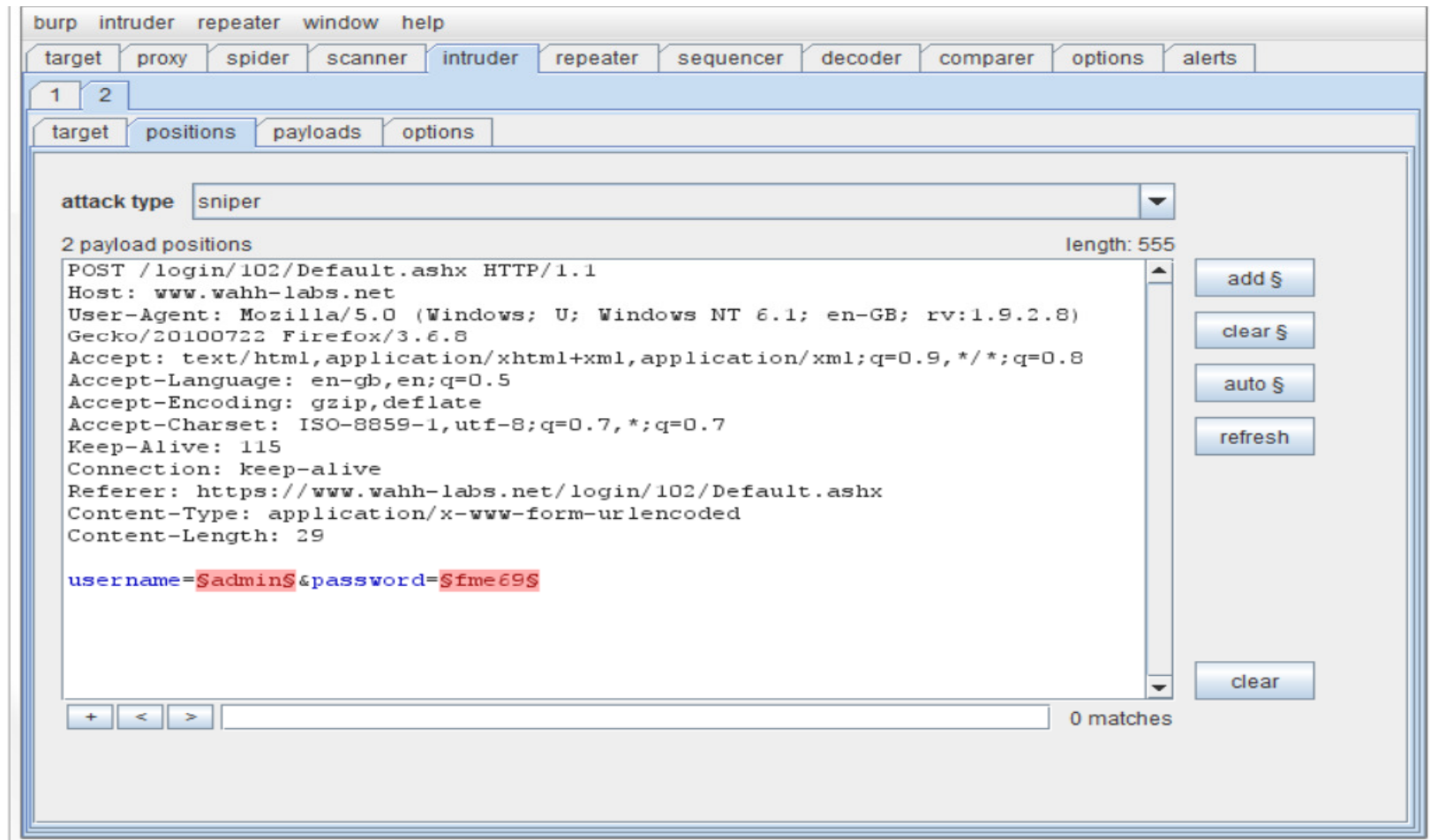
Burp Target tab:

- ❖ This tab is used to configure the details of the target server: The "host" field is used to specify the IP address or hostname of the target server. The "port" field is used to specify the port number of the HTTP/S service. The "use SSL" box is used to specify whether Secure Sockets Layer connections should be used.



Burp Intruder - Positions tab

- Position tab is used to configure the template for all the HTTP requests generated in the attack.



Burp Intruder – Payloads tab

- ❖ This tab is used to configure one or more sets of payloads. If the "pitchfork" or "cluster bomb" attack types are defined (see Positions tab) then a separate payload set must be configured for each defined payload position (up to a maximum of 8). Use the "payload set" drop-down menu to select which payload set to configure.

The screenshot shows the 'payload set' configuration window in Burp Intruder. At the top, there is a 'payload set' dropdown menu set to '1' and a 'preset list' dropdown menu. Below these is a large text area containing the following text: `'`, `"`, `../../../../../../etc/passwd`, and `<script>alert(document.cookie)</script>`. To the right of the text area are several buttons: 'add', 'add from list ...', 'load ...', 'delete', 'paste', and 'clear'. The 'add' button is next to an empty text input field. The 'add from list ...' button is next to a dropdown menu.

Burp Intruder Uses:

- Performing fuzzing of application requests to identify common vulnerabilities, such as SQL injection, cross-site scripting, and buffer overflows.
- Deliver customized brute-force attacks against authentication schemes and session handling mechanisms.



Burp Repeater

- Burp Repeater is a tool for manually modifying and reissuing individual HTTP requests, and analysing their responses. It is best used in conjunction with the other Burp Suite tools.

The screenshot shows the Burp Suite Repeater window. The top menu bar includes 'burp', 'intruder', 'repeater', 'window', and 'help'. Below the menu bar are tabs for 'target', 'proxy', 'spider', 'scanner', 'intruder', 'repeater', 'sequencer', 'decoder', 'comparer', 'comms', and 'alerts'. The 'repeater' tab is active. Below the tabs are 'intercept', 'options', and 'history' buttons. A filter bar shows 'Filter: hiding CSS, image and general binary content'. The main table lists HTTP requests with columns: #, host, method, URL, params, mod, status, length, MIME type, extension, title, SSL, and port. The selected request is #247, a GET request to 'http://www.amazon.com/s/ref=nb_ss_b?url=search-alias%3Daps&field-keywords=web+application+hacker%27s+handbook&x=8&y=19'. A context menu is open over this request, showing options like 'add item to scope', 'remove item from scope', 'spider from here', 'actively scan this item', 'passively scan this item', 'send to intruder', 'send to repeater', 'send to sequencer', 'send to comparer (request)', 'send to comparer (response)', 'delete this item', 'copy URL', and 'copy links in item'. The bottom section shows the 'request' tab with 'raw', 'params', 'headers', and 'hex' sub-tabs. The 'raw' tab is active, showing the raw HTTP request text.

#	host	method	URL	params	mod	status	length	MIME type	extension	title	SSL	port
191	http://ad.doubleclick.net	GET	/adi/amzn.us.sr.books;sz=728x90;sn=1000;s=24;s=12...	✓	□	200	612	HTML		Click here to fin...	□	74.1
230	http://ad.doubleclick.net	GET	/adi/amzn.us.sr.books;sz=160x600;sn=1000;s=24;s=1...	✓	□	200	963	HTML		Click here to fin...	□	74.1
231	http://uac.advertising.com	GET	/wrapper/aceUAC.js	✓	□	200	13058	script	js		□	213.
237	http://r1.beta.ace.advertis...	GET	/site=756290/size=728090/u=1/bnum=88761/hr=16/hl...	✓	□	200	1907	HTML			□	64.2
238	http://altfarm.mediaplex.c...	GET	/ad/js/10236-67622-17214-1?mpt=7105022&mpvc=htt...	✓	□	200	535	script			□	64.1
239	http://ad.uk.doubleclick.net	GET	/adi/N1238.Adcom.quantum/B3015474.2;sz=728x90;cl...	✓	□	200	3360	HTML	2	Click here to fin...	□	209.
247	http://www.amazon.com	GET	/s/ref=nb_ss_b?url=search-alias%3Daps&field-keywo...	✓	□	200	228525	HTML		Amazon.com: w...	□	207.
248	http://ad.doubleclick.net	GET	/adi/amzn.us.sr.aps;sz=160x600;sn=507846;s=2...	✓	□	200	612	HTML		Click here to fin...	□	74.1
252	http://ad.doubleclick.net	GET	/adi/amzn.us.sr.aps;sz=728x90;sn=507846;s=24...	✓	□	200	963	HTML		Click here to fin...	□	74.1
256	http://altfarm.mediaplex.c...	GET	/ad/js/10236-67622-17214-1?mpt=3125803&mp...	✓	□	200	535	script			□	64.1
257	http://uac.advertising.com	GET	/wrapper/aceUAC.js	✓	□	200	13058	script	js		□	213.
258	http://r1.beta.ace.advertis...	GET	/site=756290/size=728090/u=1/bnum=80511434...	✓	□	200	1907	HTML			□	64.2
259	http://ad.uk.doubleclick.net	GET	/adi/N1238.Adcom.quantum/B3015474.2;sz=728...	✓	□	200	3360	HTML	2	Click here to fin...	□	209.

request response

raw params headers hex

GET request to /s/ref=nb_ss_b

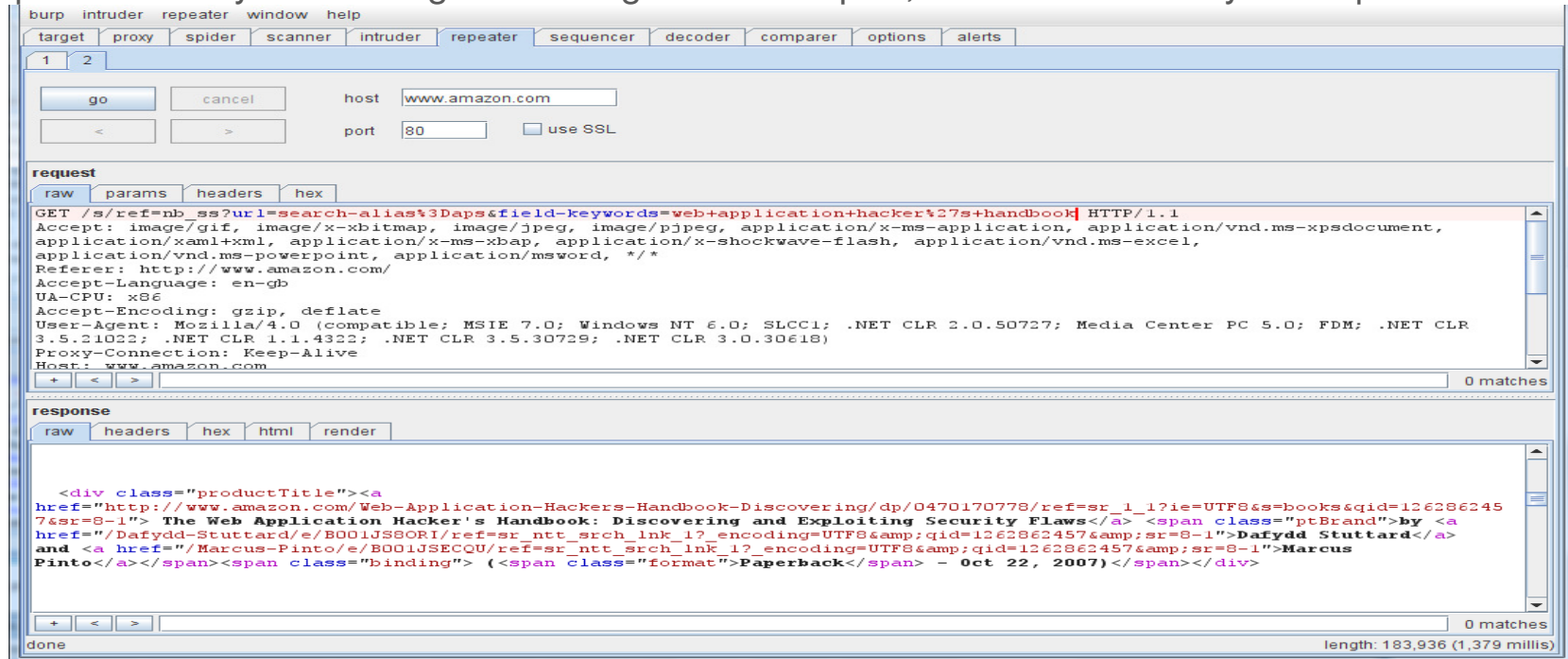
type	name	value
URL	url	search-alias%3Daps
URL	field-keywords	web+application+hacker%27s+handbook
URL	x	8
URL	y	19
cookie	session-id-time	1320444400

body encoding:



Burp Repeater Contd...

- When you send a request to Repeater from another tool, that request gets its own tab. Each tab has its own request and response windows, and its own history. The top half of the panel allows you to configure the target host and port, and the details of your request.



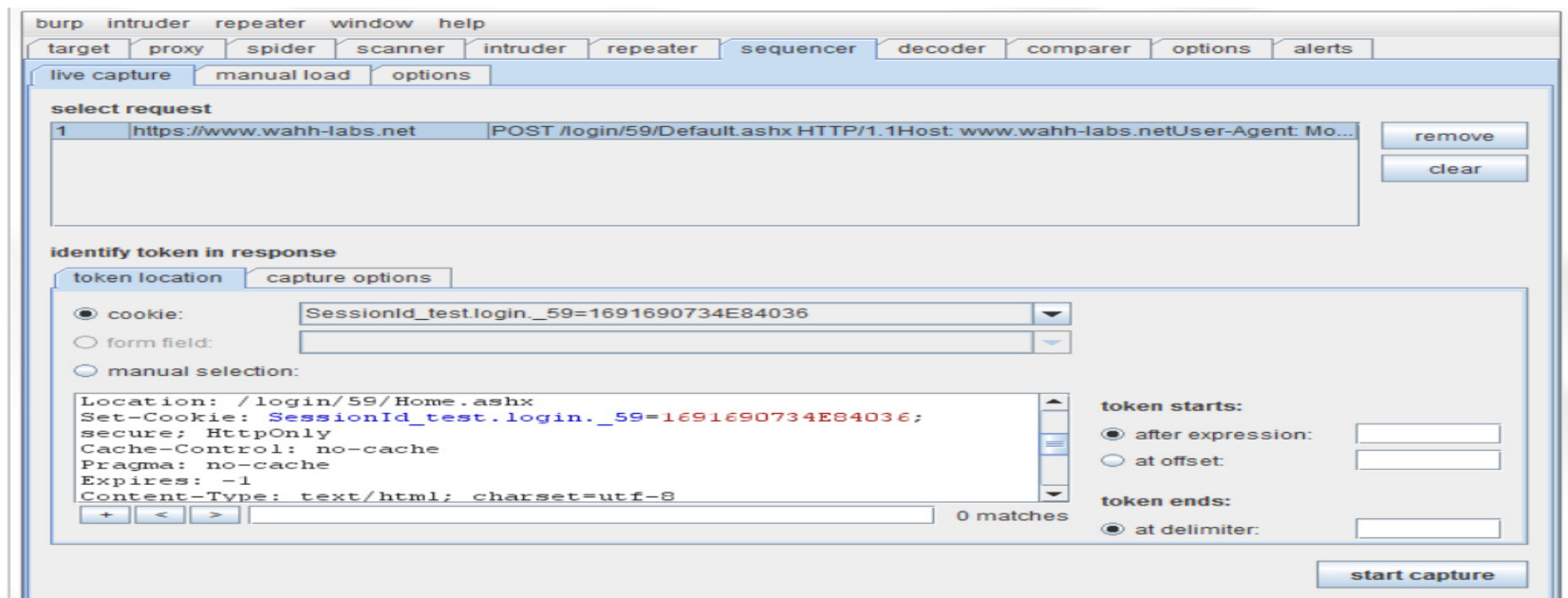
➤ Burp Repeater Uses:

- ❖ Send requests from other Burp Suite tools to test manually in Burp Repeater.
- ❖ Repeatedly change and resubmit the same request, and review the response.



Burp Sequencer

- Burp Sequencer is a tool for analyzing the degree of randomness in security-critical tokens issued by an application. It is typically used to test the quality of an application's session tokens or other items, such as CSRF nonces, on whose unpredictability the application depends for its security



➤ Burp Sequencer Uses:

- ❖ Send requests that return a security token from other Burp Suite tools to test in Burp Sequencer.
- ❖ Reissue the same request repeatedly, to generate a large sample of tokens



Conclusion

- Burp is easy to use and intuitive, allowing new users to begin working right away. Burp is also highly configurable, and contains numerous powerful features to assist the most experienced testers with their work.
- Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.



Questions?





Thank You!!

