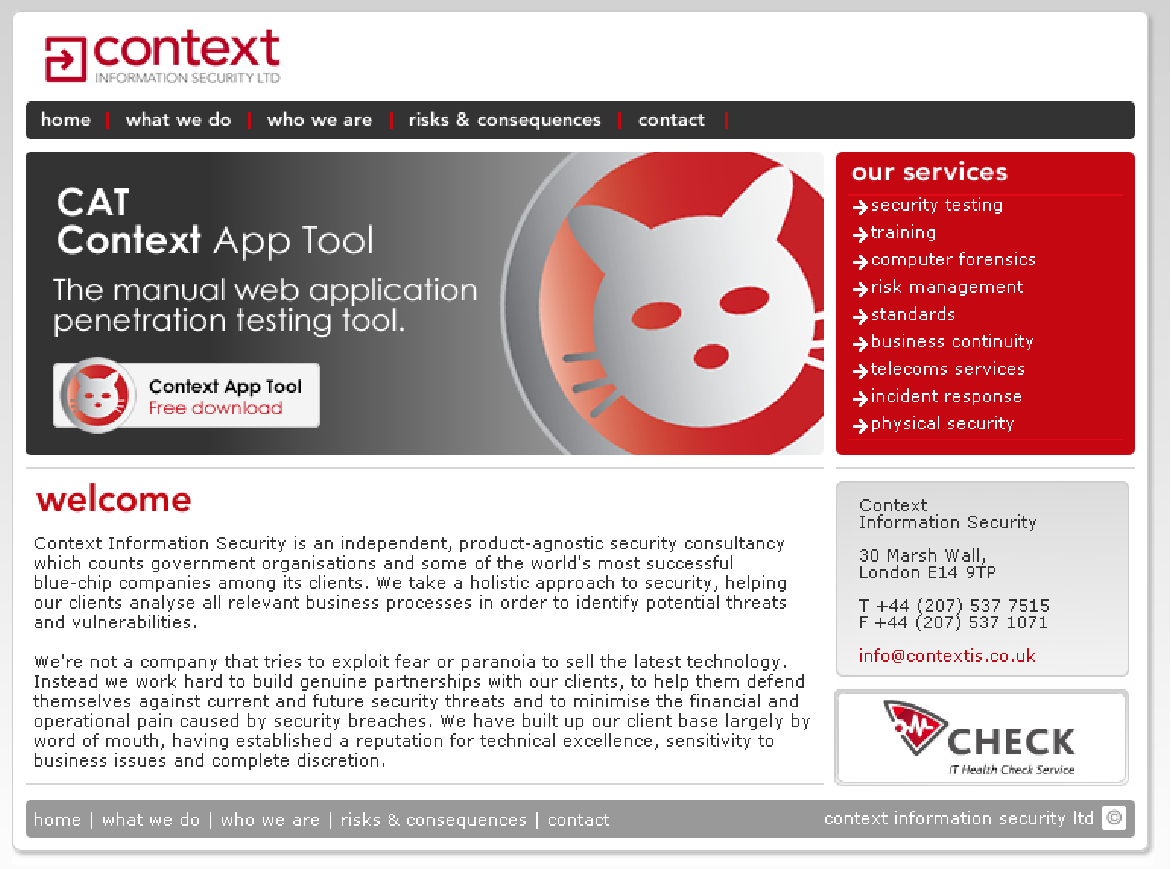
CAT

Context Information Security Ltd

December 2009 / Michael Jordon

CAT

CAT Web Site


context
INFORMATION SECURITY LTD
home | what we do | who we are | risks & consequences | contact |
Context App Tool
Free download

CAT
Context App Tool

The manual web application penetration testing tool.

our services

- security testing
- training
- computer forensics
- risk management
- standards
- business continuity
- telecoms services
- incident response
- physical security

welcome

Context Information Security is an independent, product-agnostic security consultancy which counts government organisations and some of the world's most successful blue-chip companies among its clients. We take a holistic approach to security, helping our clients analyse all relevant business processes in order to identify potential threats and vulnerabilities.

We're not a company that tries to exploit fear or paranoia to sell the latest technology. Instead we work hard to build genuine partnerships with our clients, to help them defend themselves against current and future security threats and to minimise the financial and operational pain caused by security breaches. We have built up our client base largely by word of mouth, having established a reputation for technical excellence, sensitivity to business issues and complete discretion.

Context
Information Security

30 Marsh Wall,
London E14 9TP

T +44 (207) 537 7515
F +44 (207) 537 1071

info@contextis.co.uk

CHECK
IT Health Check Service
home | what we do | who we are | risks & consequences | contact
context information security ltd ©

http://cat.contextis.com

CAT Context Application Tool

- Manual Application Testing Tool
- Lead Developer: Michael Jordon – Crest App Cert
- Contains:
  - Inline Proxy
  - Repeater
  - Fuzzer
  - Log
  - Authentication Checker
  - SSL Checker
  - Notepad
  - Browser

http://cat.contextis.com

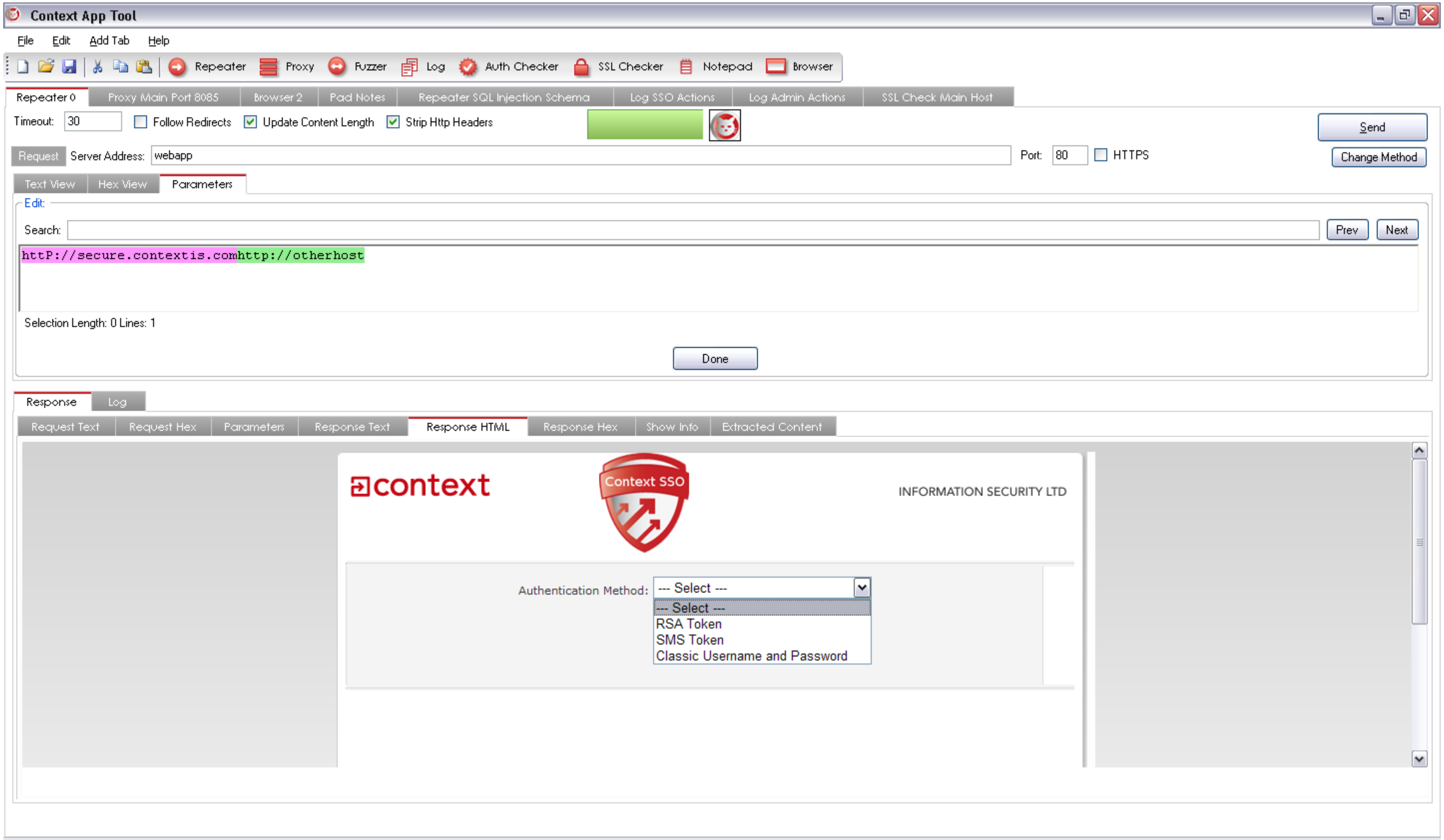
History

- Started Development 2007
- Context's Core application testing tool
- Collaborative Effort within Context
  - Features fed from Context's Experience

Why another tool?

- Frustration
  - Why doesn’t this render the HTML correctly!
  - Authorisation Checking is a pain in the ****
  - Tool should make your life easier not harder
  - All this copy and pasting makes me feel like a machine
- Complex Systems
  - SSO
  - CSRF Tokens
  - Timing Attacks
  - Web Services
  - ….

CAT Demo



Timeout: 30 □ Follow Redirects ☑ Update Content Length ☑ Strip Http Headers

Server Address: webapp Port: 80 □ HTTPS

Search:

```
httP://secure.contextis.comhttp://otherhost
```

Selection Length: 0 Lines: 1

Authentication Method: --- Select ---

- --- Select ---
- RSA Token
- SMS Token
- Classic Username and Password

Future

- Currently Beta 4
- Next Version later this year
- Possible Major Features for V1.1
  - Auth Checker with Integrated Browsers
  - More auto testers
  - Full Ajax Spider
  - Combine Fuzzer/Log/Repeater
  - …

Future

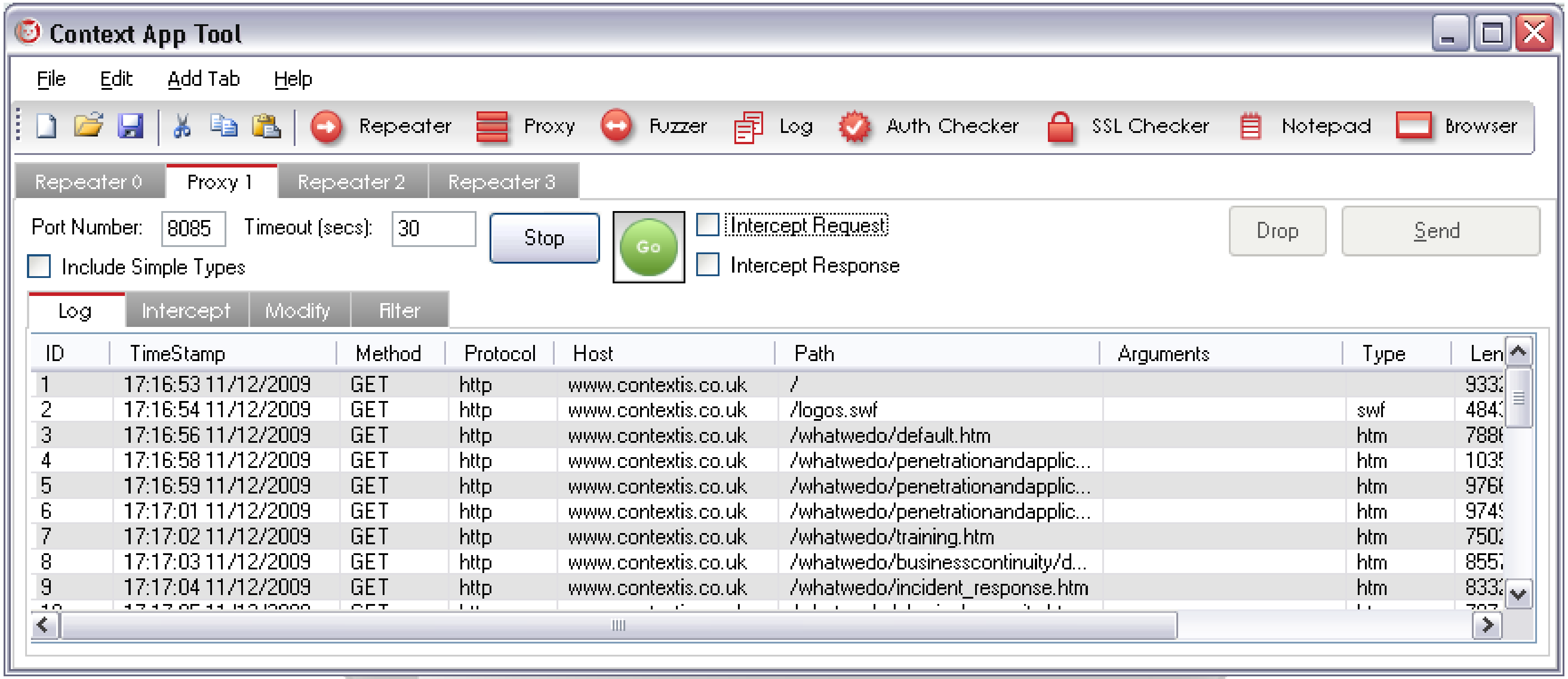
- Looking for Contributions
  - – Bugs
  - – Ideas
  - – Feature Requests

cat@contextis.com

http://cat.contextis.com

CAT

Proxy



Port Number: 8085 Timeout (secs): 30

□ Include Simple Types

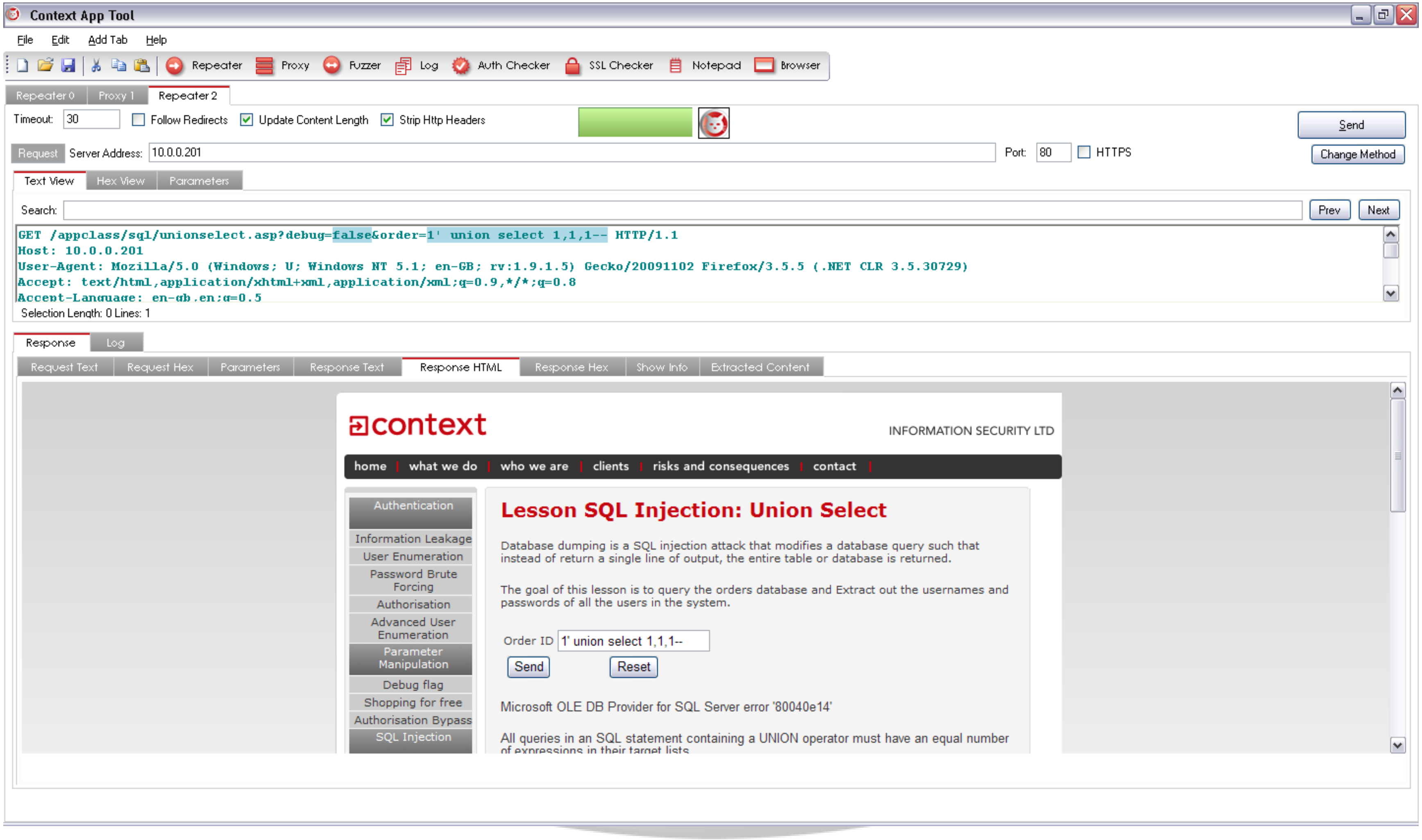
□ Intercept Request

□ Intercept Response

ID	TimeStamp	Method	Protocol	Host	Path	Arguments	Type	Len
1	17:16:53 11/12/2009	GET	http	www.contextis.co.uk	/			933
2	17:16:54 11/12/2009	GET	http	www.contextis.co.uk	/logos.swf		swf	484
3	17:16:56 11/12/2009	GET	http	www.contextis.co.uk	/whatwedo/default.htm		htm	788
4	17:16:58 11/12/2009	GET	http	www.contextis.co.uk	/whatwedo/penetrationandapplic...		htm	103
5	17:16:59 11/12/2009	GET	http	www.contextis.co.uk	/whatwedo/penetrationandapplic...		htm	976
6	17:17:01 11/12/2009	GET	http	www.contextis.co.uk	/whatwedo/penetrationandapplic...		htm	974
7	17:17:02 11/12/2009	GET	http	www.contextis.co.uk	/whatwedo/training.htm		htm	750
8	17:17:03 11/12/2009	GET	http	www.contextis.co.uk	/whatwedo/businesscontinuity/d...		htm	855
9	17:17:04 11/12/2009	GET	http	www.contextis.co.uk	/whatwedo/incident_response.htm		htm	833

CAT

Repeater



Timeout: 30 □ Follow Redirects ☑ Update Content Length ☑ Strip Http Headers

Server Address: 10.0.0.201 Port: 80 □ HTTPS

```
GET /appclass/sql/unionselect.asp?debug=false&order=1' union select 1,1,1-- HTTP/1.1
Host: 10.0.0.201
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
```

Selection Length: 0 Lines: 1

Lesson SQL Injection: Union Select

Database dumping is a SQL injection attack that modifies a database query such that instead of return a single line of output, the entire table or database is returned.

The goal of this lesson is to query the orders database and Extract out the usernames and passwords of all the users in the system.

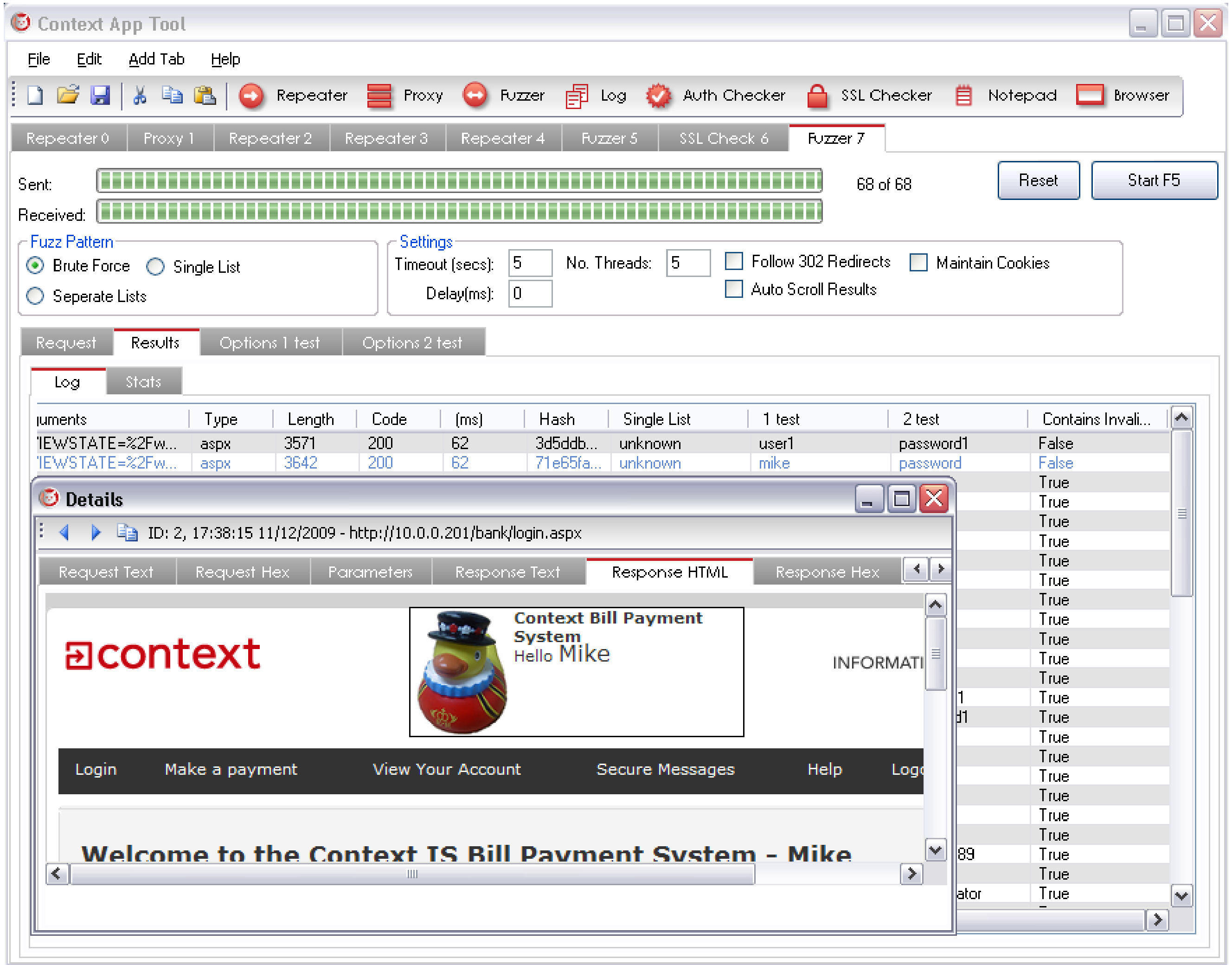
Order ID 1' union select 1,1,1--

Microsoft OLE DB Provider for SQL Server error '80040e14'

All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists

CAT

Fuzzer



Sent: 68 of 68

Received:

Fuzz Pattern

● Brute Force ○ Single List

○ Seperate Lists

Settings

Timeout (secs): 5 No. Threads: 5 □ Follow 302 Redirects □ Maintain Cookies

Delay(ms): 0 □ Auto Scroll Results

uments	Type	Length	Code	(ms)	Hash	Single List	1 test	2 test	Contains Invali...
IEWSTATE=%2Fw...	aspx	3571	200	62	3d5ddb...	unknown	user1	password1	False
IEWSTATE=%2Fw...	aspx	3642	200	62	71e65fa...	unknown	mike	password	False
									True
									True
									True
									True
									True
									True
									True
									True
									True
									True
									True
								1	True
								d1	True
									True
									True
									True
									True
									True
									True
								89	True
									True
								ator	True

Details

ID: 2, 17:38:15 11/12/2009 - http://10.0.0.201/bank/login.aspx

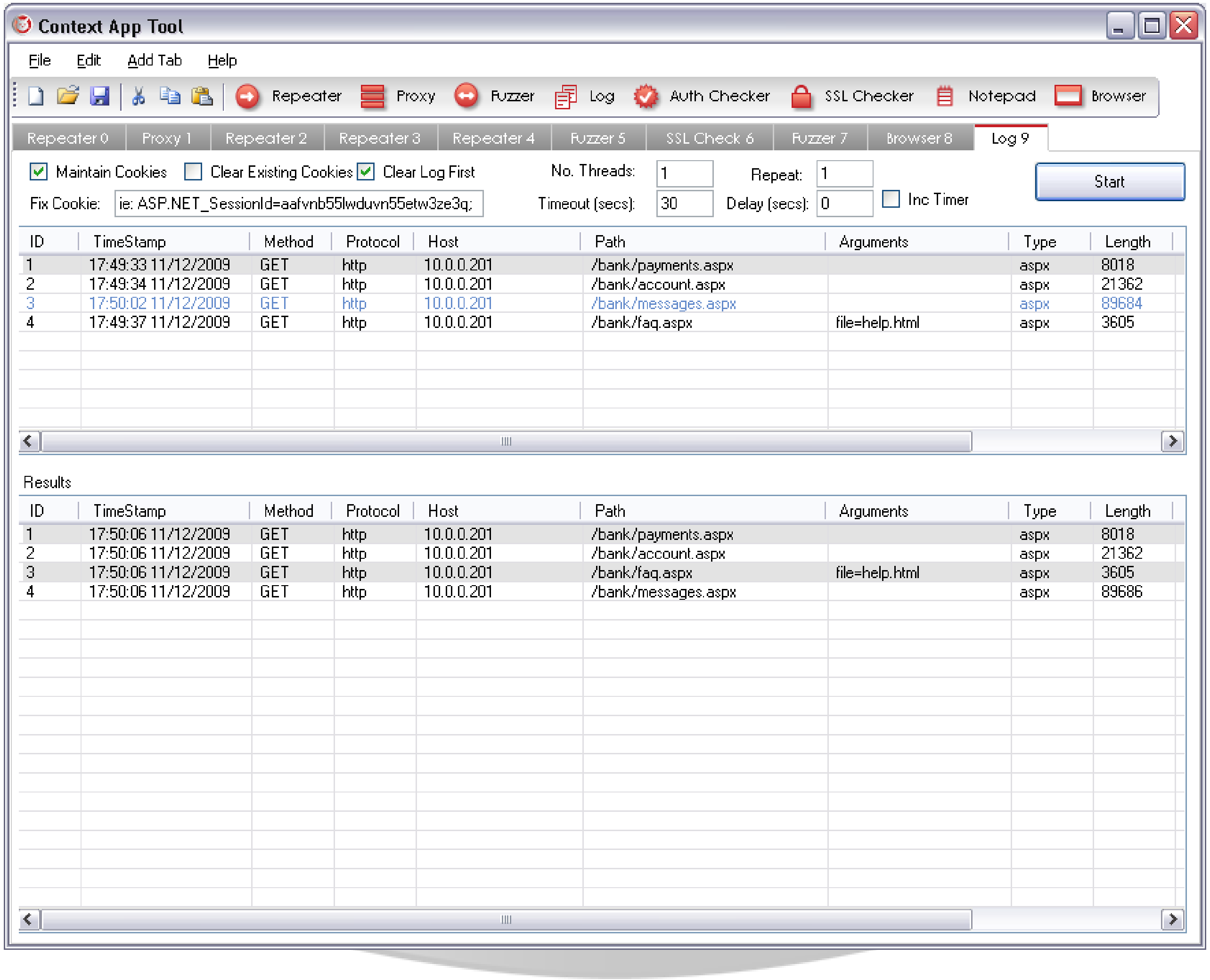
Context Bill Payment System

Hello Mike

Welcome to the Context IS Bill Payment System - Mike

CAT

Log



☑ Maintain Cookies ☐ Clear Existing Cookies ☑ Clear Log First

No. Threads: 1 Repeat: 1

Fix Cookie: ie: ASP.NET_SessionId=aafvnb55lwduvn55etw3ze3q;

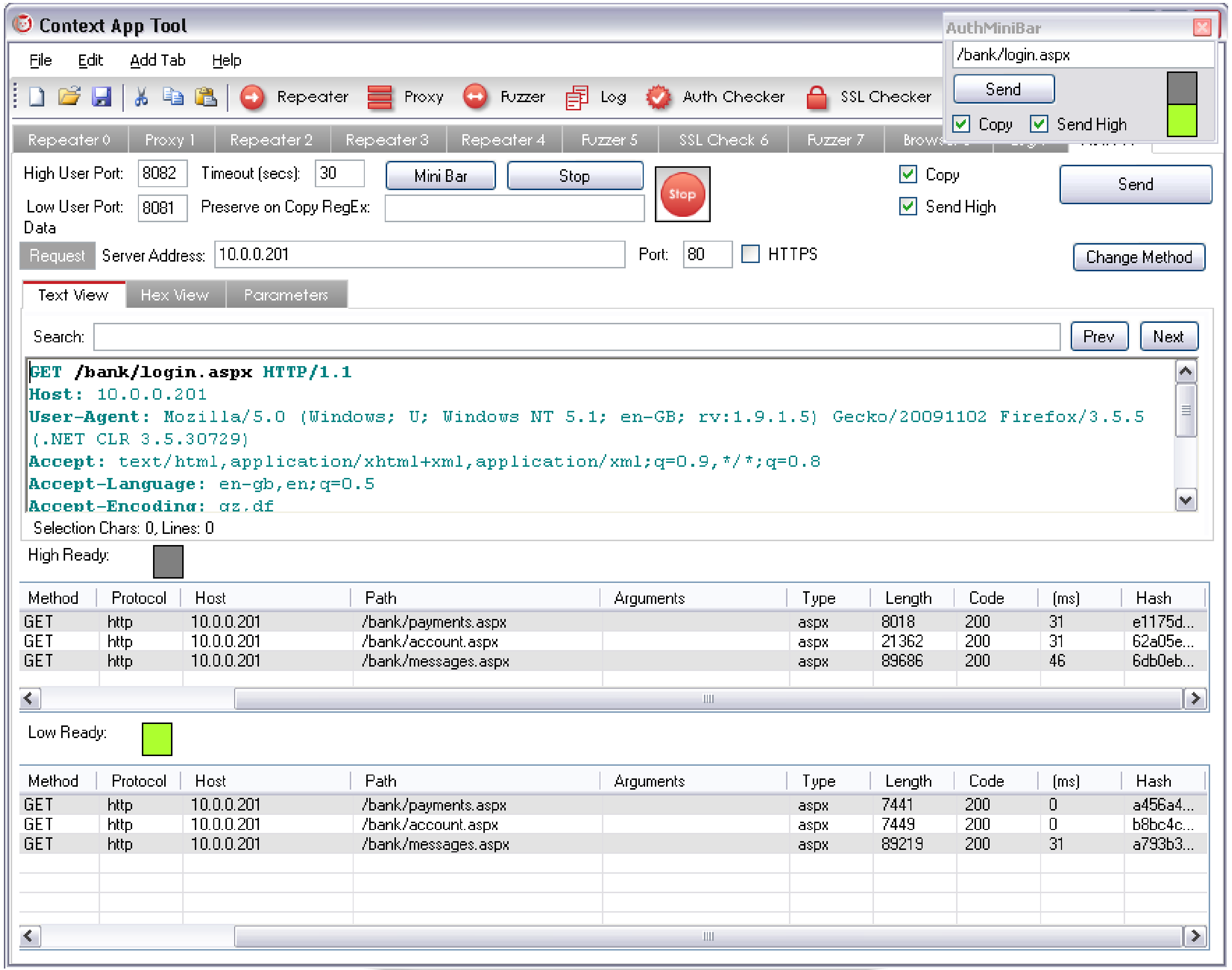
Timeout (secs): 30 Delay (secs): 0 ☐ Inc Timer

ID	TimeStamp	Method	Protocol	Host	Path	Arguments	Type	Length
1	17:49:33 11/12/2009	GET	http	10.0.0.201	/bank/payments.aspx		aspx	8018
2	17:49:34 11/12/2009	GET	http	10.0.0.201	/bank/account.aspx		aspx	21362
3	17:50:02 11/12/2009	GET	http	10.0.0.201	/bank/messages.aspx		aspx	89684
4	17:49:37 11/12/2009	GET	http	10.0.0.201	/bank/faq.aspx	file=help.html	aspx	3605

Results

ID	TimeStamp	Method	Protocol	Host	Path	Arguments	Type	Length
1	17:50:06 11/12/2009	GET	http	10.0.0.201	/bank/payments.aspx		aspx	8018
2	17:50:06 11/12/2009	GET	http	10.0.0.201	/bank/account.aspx		aspx	21362
3	17:50:06 11/12/2009	GET	http	10.0.0.201	/bank/faq.aspx	file=help.html	aspx	3605
4	17:50:06 11/12/2009	GET	http	10.0.0.201	/bank/messages.aspx		aspx	89686

Auth Checker


Context App Tool
File Edit Add Tab Help
Repeater Proxy Fuzzer Log Auth Checker SSL Checker
Repeater 0 | Proxy 1 | Repeater 2 | Repeater 3 | Repeater 4 | Fuzzer 5 | SSL Check 6 | Fuzzer 7 | Brows
AuthMiniBar
Send
Mini Bar
Stop
Stop
Send
Change Method
Data
Request
Text View | Hex View | Parameters
Prev
Next

AuthMiniBar: /bank/login.aspx

☑ Copy ☑ Send High

High User Port: 8082 Timeout (secs): 30

Low User Port: 8081 Preserve on Copy RegEx:

☑ Copy

☑ Send High

Server Address: 10.0.0.201 Port: 80 □ HTTPS

Search:

```
GET /bank/login.aspx HTTP/1.1
Host: 10.0.0.201
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
(.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gz.df
```

Selection Chars: 0, Lines: 0

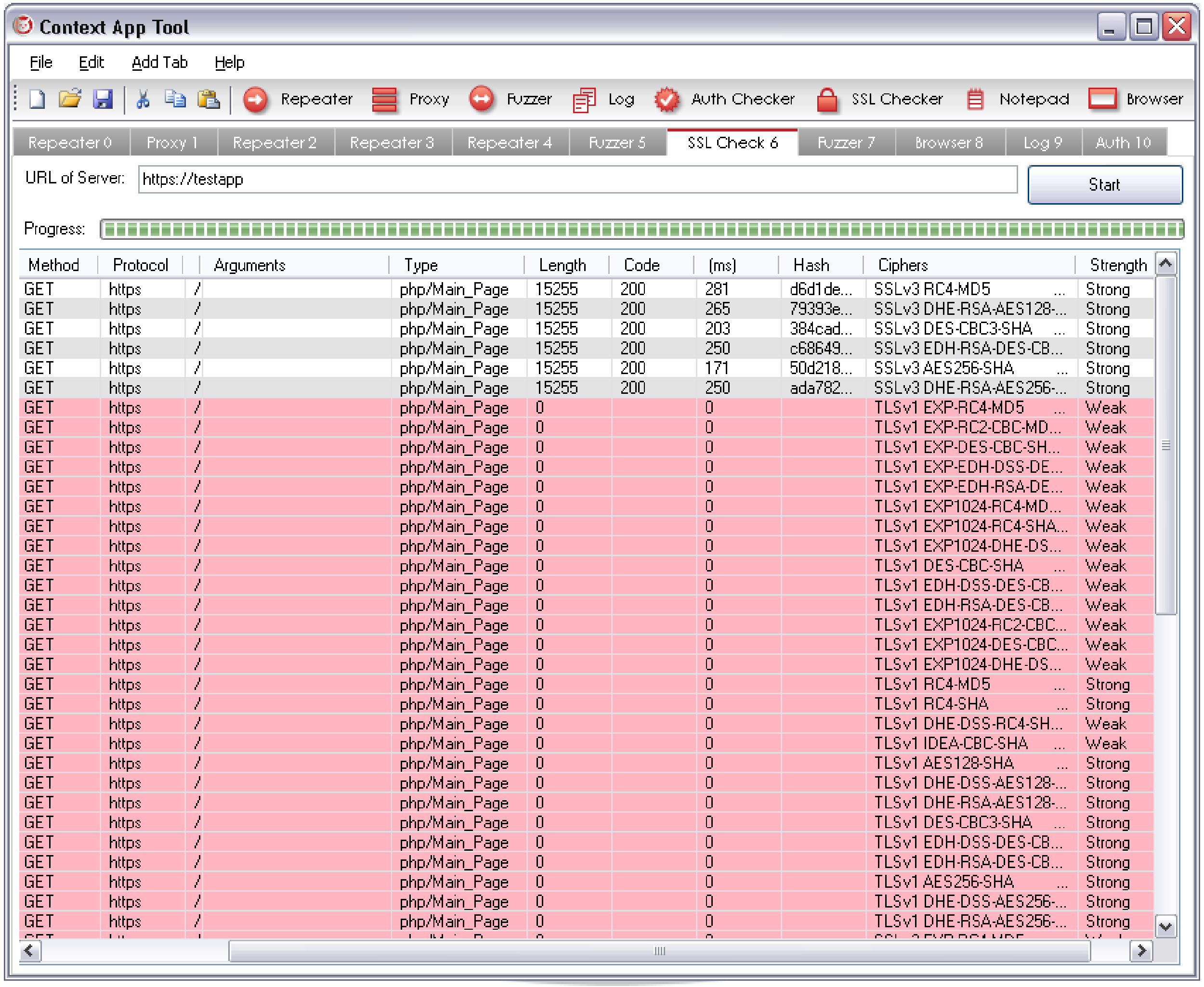
High Ready:

Method	Protocol	Host	Path	Arguments	Type	Length	Code	(ms)	Hash
GET	http	10.0.0.201	/bank/payments.aspx		aspx	8018	200	31	e1175d...
GET	http	10.0.0.201	/bank/account.aspx		aspx	21362	200	31	62a05e...
GET	http	10.0.0.201	/bank/messages.aspx		aspx	89686	200	46	6db0eb...

Low Ready:

Method	Protocol	Host	Path	Arguments	Type	Length	Code	(ms)	Hash
GET	http	10.0.0.201	/bank/payments.aspx		aspx	7441	200	0	a456a4...
GET	http	10.0.0.201	/bank/account.aspx		aspx	7449	200	0	b8bc4c...
GET	http	10.0.0.201	/bank/messages.aspx		aspx	89219	200	31	a793b3...

SSL Checker

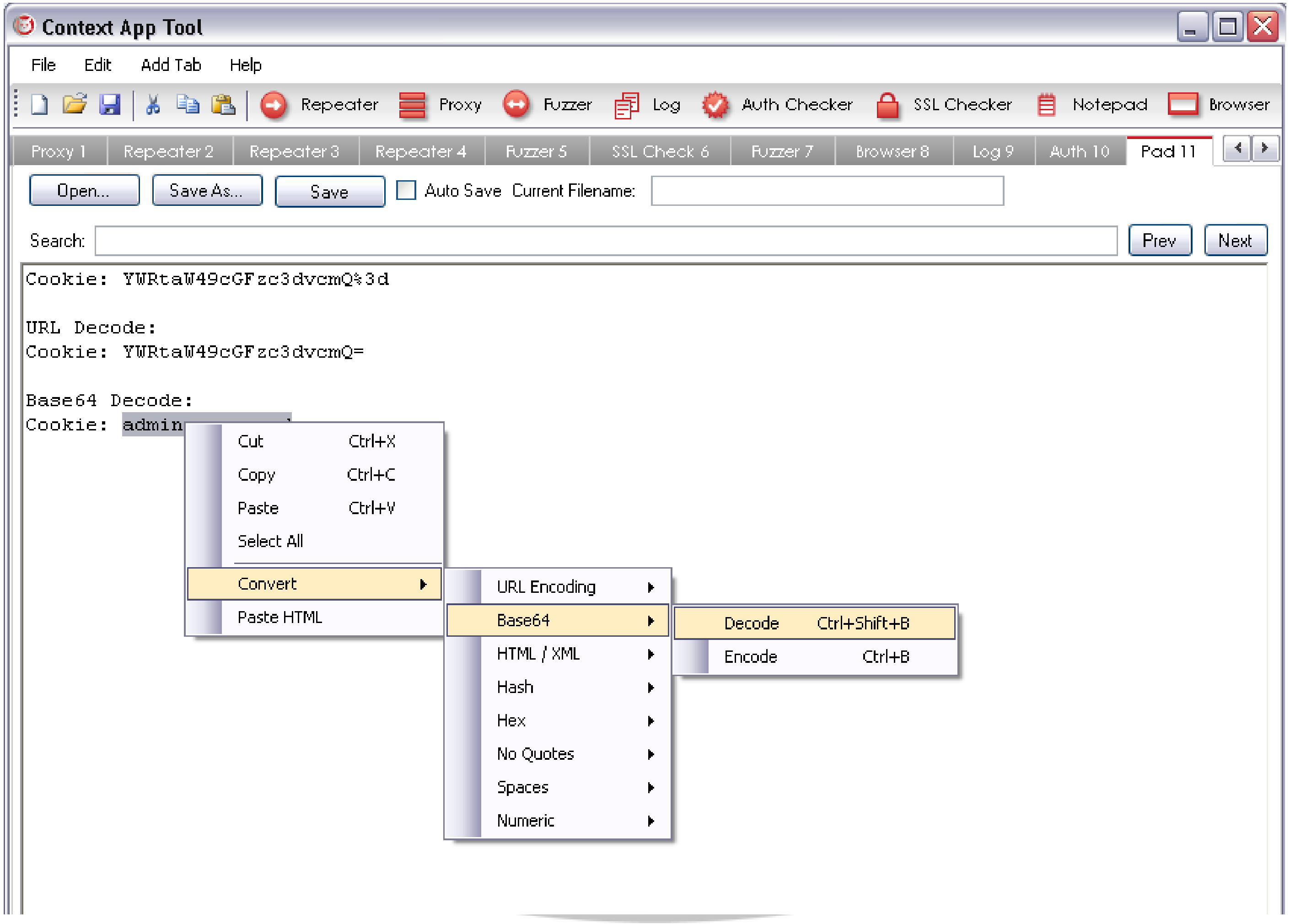


URL of Server: https://testapp

Progress:

Method	Protocol		Arguments	Type	Length	Code	(ms)	Hash	Ciphers	Strength
GET	https	/		php/Main_Page	15255	200	281	d6d1de...	SSLv3 RC4-MD5 ...	Strong
GET	https	/		php/Main_Page	15255	200	265	79393e...	SSLv3 DHE-RSA-AES128-...	Strong
GET	https	/		php/Main_Page	15255	200	203	384cad...	SSLv3 DES-CBC3-SHA ...	Strong
GET	https	/		php/Main_Page	15255	200	250	c68649...	SSLv3 EDH-RSA-DES-CB...	Strong
GET	https	/		php/Main_Page	15255	200	171	50d218...	SSLv3 AES256-SHA ...	Strong
GET	https	/		php/Main_Page	15255	200	250	ada782...	SSLv3 DHE-RSA-AES256-...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 EXP-RC4-MD5 ...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP-RC2-CBC-MD...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP-DES-CBC-SH...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP-EDH-DSS-DE...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP-EDH-RSA-DE...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP1024-RC4-MD...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP1024-RC4-SHA...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP1024-DHE-DS...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 DES-CBC-SHA ...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EDH-DSS-DES-CB...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EDH-RSA-DES-CB...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP1024-RC2-CBC...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP1024-DES-CBC...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 EXP1024-DHE-DS...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 RC4-MD5 ...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 RC4-SHA ...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 DHE-DSS-RC4-SH...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 IDEA-CBC-SHA ...	Weak
GET	https	/		php/Main_Page	0		0		TLSv1 AES128-SHA ...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 DHE-DSS-AES128-...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 DHE-RSA-AES128-...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 DES-CBC3-SHA ...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 EDH-DSS-DES-CB...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 EDH-RSA-DES-CB...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 AES256-SHA ...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 DHE-DSS-AES256-...	Strong
GET	https	/		php/Main_Page	0		0		TLSv1 DHE-RSA-AES256-...	Strong

Notepad

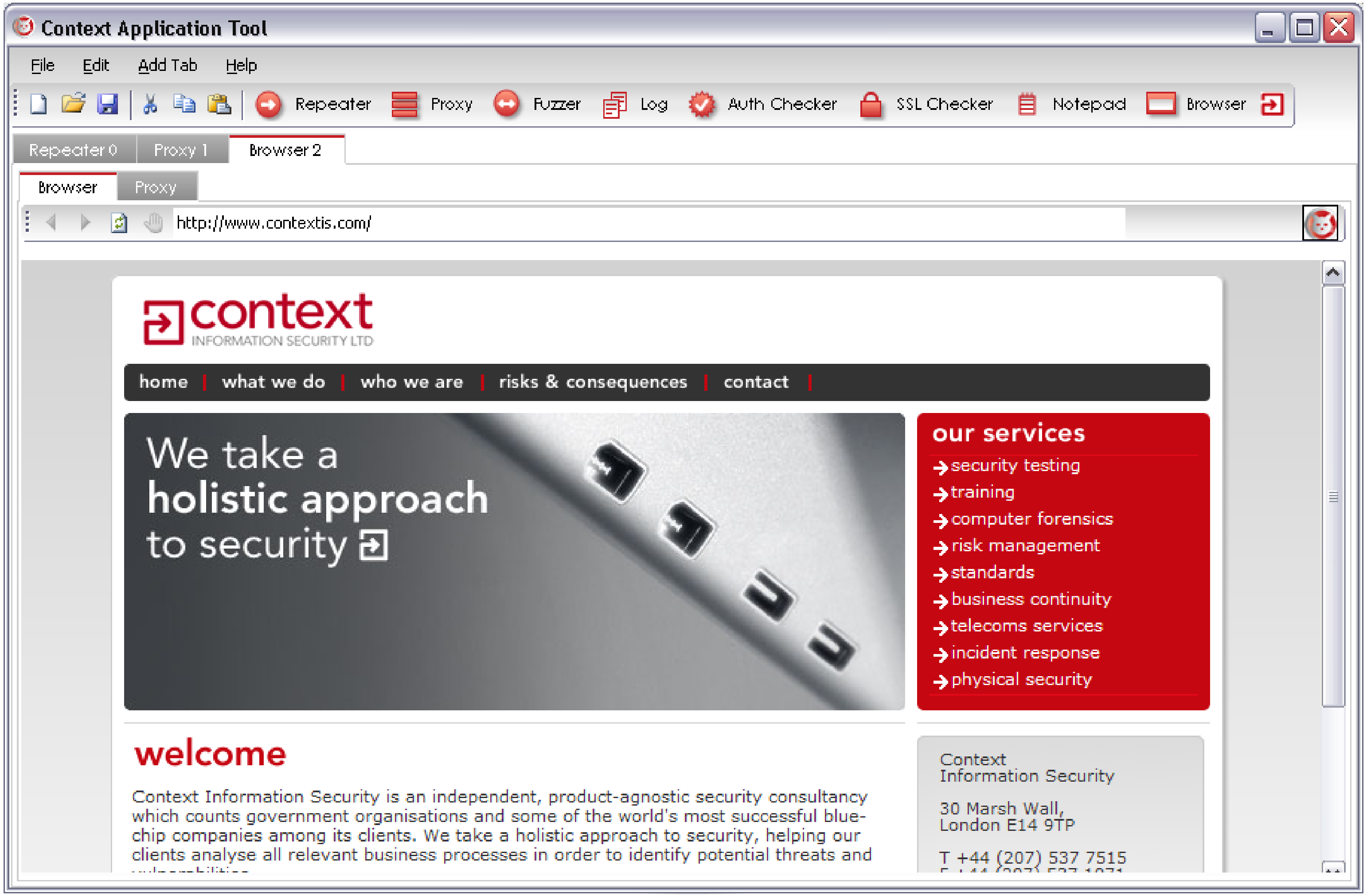


```
Cookie: YWRtaW49cGFzc3dvcmQ%3d

URL Decode:
Cookie: YWRtaW49cGFzc3dvcmQ=

Base64 Decode:
Cookie: admin
```

Web Browser



We take a holistic approach to security

our services

- security testing
- training
- computer forensics
- risk management
- standards
- business continuity
- telecoms services
- incident response
- physical security

welcome

Context Information Security is an independent, product-agnostic security consultancy which counts government organisations and some of the world's most successful blue-chip companies among its clients. We take a holistic approach to security, helping our clients analyse all relevant business processes in order to identify potential threats and vulnerabilities

Context
Information Security

30 Marsh Wall,
London E14 9TP

T +44 (207) 537 7515