

Web Hacking

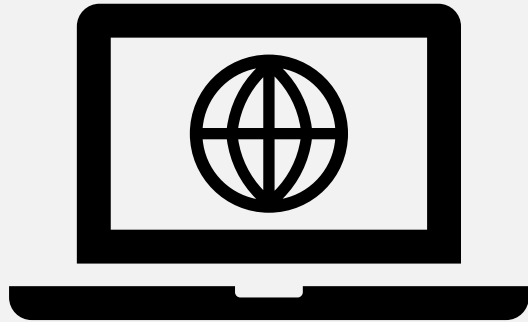
CONTENTS

Contents 1

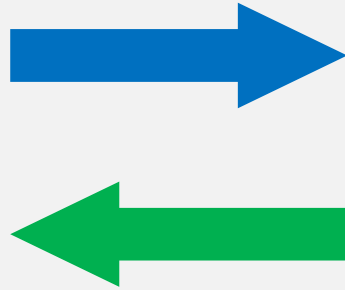
- GET & POST
- http
- Proxy

Contents 1
GET & POST

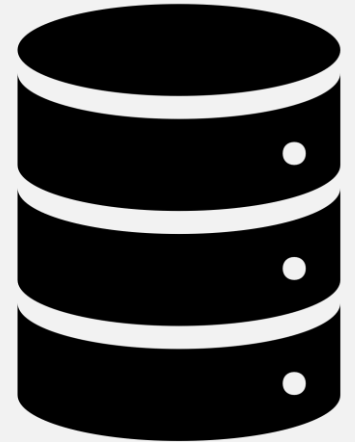
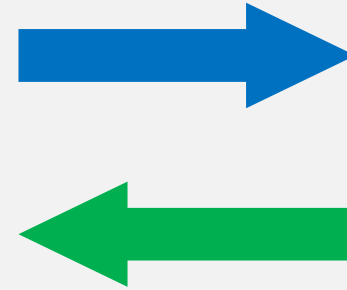
http



Client

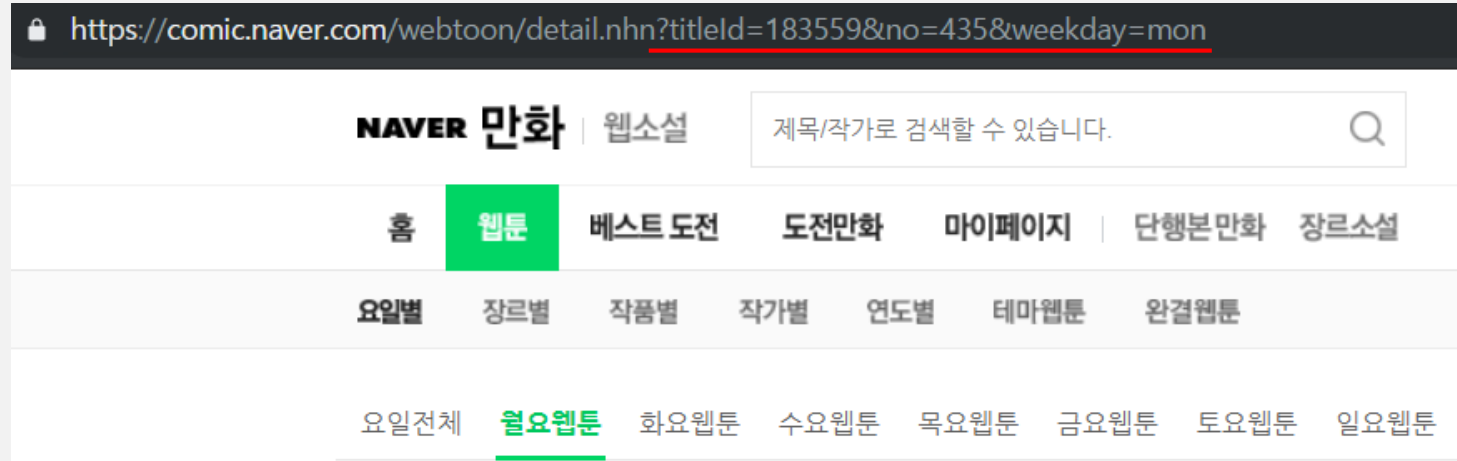


Server



Database

GET Method



- 인자가 URL의 ? 뒤에 붙어서 전달
titleId, no, weekday 라는 인자 값이 ? 뒤에 붙어서 전달되며 각 인자는 &로 구분
- 보통 데이터를 **조회**하는 용도로 사용
위의 예시처럼 웹툰을 보거나 게시글을 보는 등의 조회 용도로 사용
- 전송하는 길이에 제한

Contents 1

GET & POST

POST Method

https://nid.naver.com/nidlogin.login

NAVER

AAAA

비밀번호

아이디 또는 비밀번호를 다시 확인하세요.
네이버에 등록되지 않은 아이디이거나, 아이디 또는 비밀번호를 잘못 입력하셨습니다.

Request Headers
POST /jsp/login/login_action.jsp HTTP/1.1

Body	
Name	Value
__E2E_RESULT__	72ba35025dbd583dcfe1e920a40a1b095be8ad9607ab268e1b488919093ab72e554365f3
__E2E_UNIQUE__	156161374923375
id__E2E__	55f12ce6c1a63347220d4c4423e12a65ce0cc1b1609ea27cf50f7867ede8bed44f21b872e8
password__E2E__	d8aca36f061710d30674a545a3703181ca7493d3f0c9efe1b92420076a00ae6dea8089c8o
rtUrl	
id	17011636
password	aaaaaaaa111aa
chkNos	on

- 인자가 URL이 아니라 **Body**에 의해 전달
URL에 노출되지 않기 때문에 보안상 조금 더 유리함
- 보통 데이터에 **영향**을 주거나 보안이 필요할 때 사용
데이터의 삭제, 수정, 삽입 등 DB에 영향을 주는 요청이거나
로그인과 같이 보안이 필요한 요청일 때 POST Method를 사용
- 전송하는 길이에 제한

Contents 1

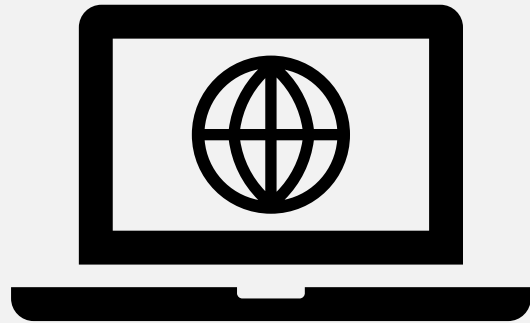
GET & POST

GET vs POST

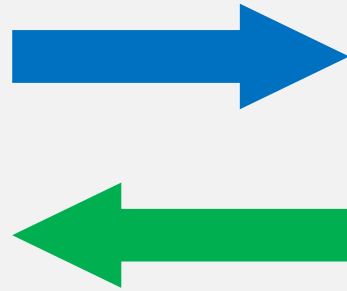
공통점	차이점	
인자를 전달하기 위한 Method이다.	GET	POST
	비교적 보안상 불리하다.	비교적 보안상 유리하다.
Client가 Server에 Request하는 Method이다.	URL을 통해 인자를 전달한다.	Body 부분에 인자를 전달한다.
	보통 데이터 조회에 사용한다.	보통 데이터 삭제, 수정, 삽입에 사용한다.

Contents 1
GET & POST

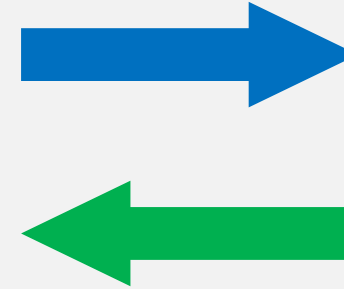
Proxy



Client



**Proxy
Server**



Server

1. 네이버 - 웹툰에서 특정 웹툰 접속

comic.naver.com/webtoon/detail.nhn?titleId=183559&no=447&weekday=mon


Google 문서 Google 프레젠테이션 Google 번역 SoundCloud - List... 보안뉴스 Index of /process OyesMall 에 오신... Home - Canva 내 드라이브 - Goo...

NAVER 만화 | 웹소설 제목/작가로 검색할 수 있습니다. 로그인

홈 **웹툰** 베스트 도전 도전만화 마이페이지 단행본만화 장르소설

요일별 장르별 작품별 작가별 연도별 테마웹툰 완결웹툰

요일전체 **월요일웹툰** 화요일웹툰 수요일웹툰 목요일웹툰 금요일웹툰 토요일웹툰 일요일웹툰

 **신의 탑** siu
자신의 모든 것이었던 소녀를 찾아 탑에 들어온 소년
그리고 그런 소년을 시험하는 탑
스토리, 판타지 | 12세 이용가

+ 관심웹툰 첫화보기 목록보기 작가의 다른 작품

3부 28화 <이전화

회별별점 ★★★★★ 9.93 (참여 12560) | 별점주기 ★★★★★ 확인

등록일 2019.09.15 | 주소복사 리모컨 ON

2. GET Method 수정

no 인자
447 -> 446 으로 변경

comic.naver.com/webtoon/detail.nhn?titleId=183559&no=447&weekday=mon

NAVER 만화 | 웹소설


제목/작가로 검색할 수 있습니다.

로그인

홈 웹툰 베스트 도전 도전만화 마이페이지 단행본만화 장르소설

요일별 장르별 작품별 작가별 연도별 테마웹툰 완결웹툰

요일전체 **월요일웹툰** 화요일웹툰 수요일웹툰 목요일웹툰 금요일웹툰 토요일웹툰 일요일웹툰

 신의 탑 siu

자신의 모든 것이었던 소녀를 좇아 탑에 들어온 소년
그리고 그런 소년을 시험하는 탑

스토리, 판타지 | 12세 이용가

+ 관심웹툰 첫화보기 목록보기 작가의 다른 작품

3부 28화 <이전화

회별별점 ★★★★★ 9.93 (참여 12560) | 별점주기 ★★★★★ 확인

등록일 2019.09.15 | 주소복사 리모컨 ON

3. 응답된 결과 확인

comic.naver.com/webtoon/detail.nhn?titleId=183559&no=446&weekday=mon


ogle 문서 Google 프레젠테이션 Google 번역 SoundCloud - List... 보안뉴스 Index of /process OyesMall 에 오신... Home - Canva 내 드라이브 - Goo...

NAVER 만화 | 웹소설 제목/작가로 검색할 수 있습니다. 로그인

홈 **웹툰** 베스트도전 도전만화 마이페이지 | 단행본만화 장르소설

요일별 장르별 작품별 작가별 연도별 테마웹툰 완결웹툰

요일전체 **월요일웹툰** 화요일웹툰 수요일웹툰 목요일웹툰 금요일웹툰 토요일웹툰 일요일웹툰

 **신의 탑** siu
자신의 모든 것이었던 소녀를 좇아 탑에 들어온 소년
그리고 그런 소년을 시험하는 탑
스토리, 판타지 | 12세 이용가

+ 관심웹툰 첫화보기 목록보기 작가의 다른 작품

3부 27화 < 이전화 > < 다음화 >

회별별점 ★★★★★ 9.97 (참여 23551) | 별점주기 ★★★★★ 확인

등록일 2019.09.08 주소복사 리모컨 ON

Contents 1

GET & POST

POST 실습

1. http://demo.testfire.net/login.jsp 접속

← → ↻ ⓘ 주의 요함 | demo.testfire.net/login.jsp

열 Google 문서 Google 프레젠테이션... Google 번역 SoundCloud - List... 보안뉴스 Index of /process OyesMall 에 오신... Home - Canva 내 드라이브 - Goo... 기타 북마크

AltoroMutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

[ONLINE BANKING LOGIN](#) [PERSONAL](#) [SMALL BUSINESS](#) [INSIDE ALTORO MUTUAL](#)

PERSONAL

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

SMALL BUSINESS

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

INSIDE ALTORO MUTUAL

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)
- [Subscribe](#)

Online Banking Login

Username:

Password:

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2019 Altoro Mutual, Inc. *This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features*

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2019, IBM Corporation, All rights reserved.

Contents 1 GET & POST

POST 실습

2. Burp Suite 가동

The screenshot displays the Burp Suite Community Edition v2.1.02 interface. The 'Proxy' tab is selected in the top navigation bar. The 'Tasks' panel on the left shows a live passive crawl from the proxy, with 816 items added to the site map and 203 responses processed. The 'Issue activity' panel on the right lists various security issues found during the scan.

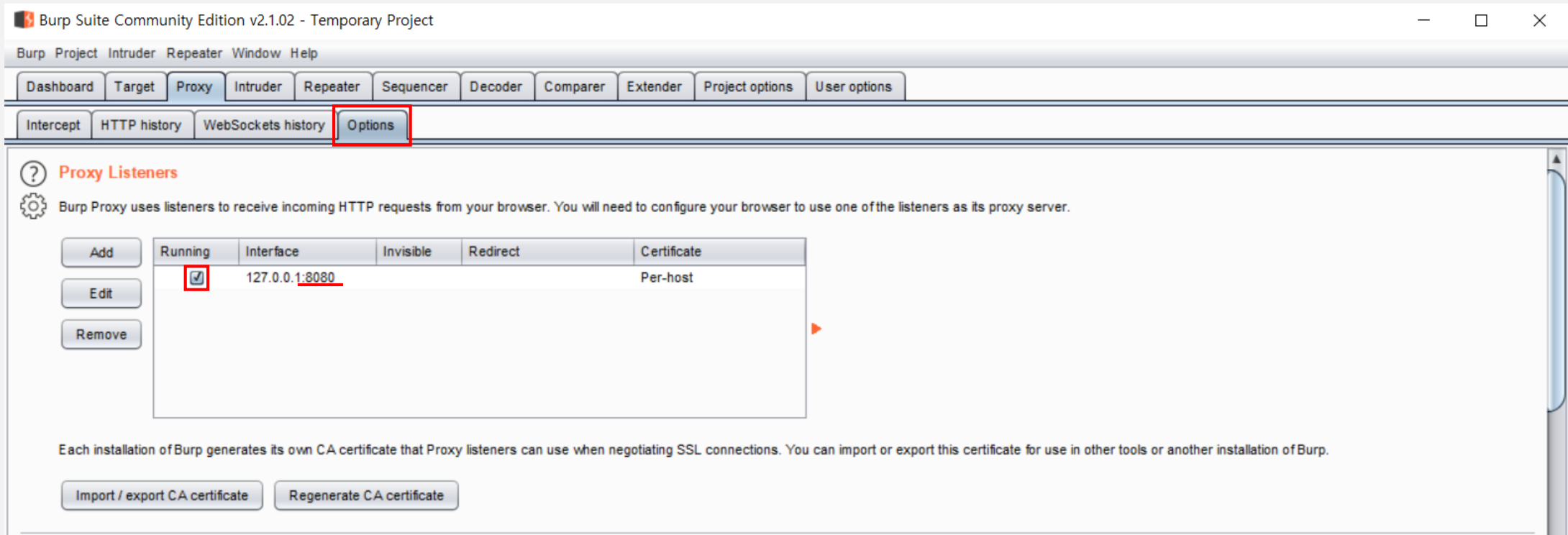
Tasks

- 1. Live passive crawl from Proxy (all traffic)
- Add links. Add item itself, same domain and URLs in suite... 816 items added to site map
- Capturing: ☒ 203 responses processed
- 0 responses queued

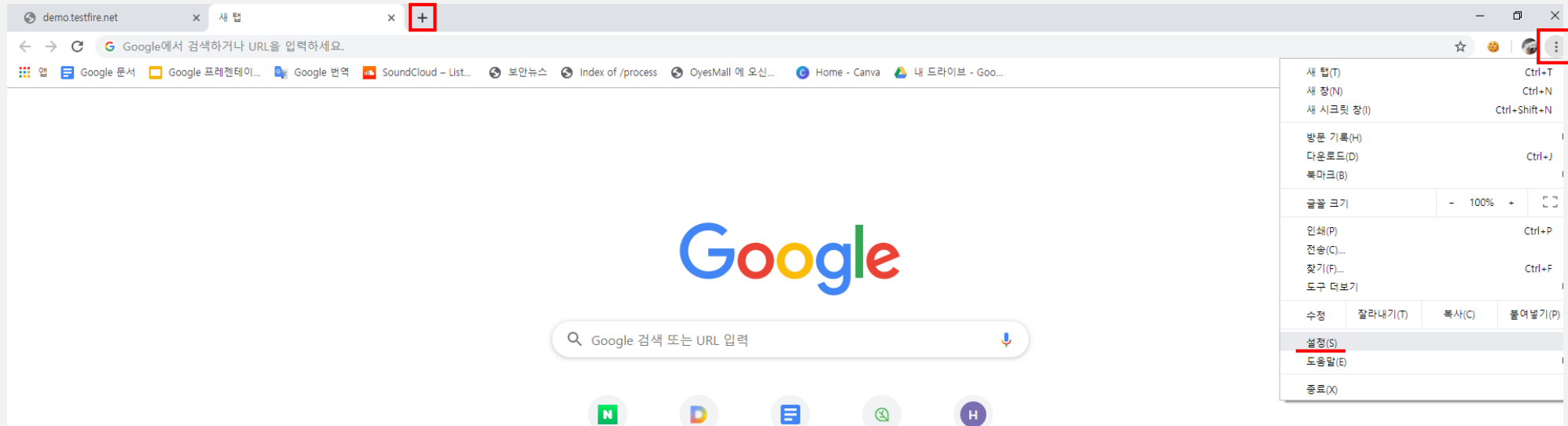
Issue activity [Pro version only]

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-website...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-website...	/
OS command injection	https://insecure-website....	/feedback/submit

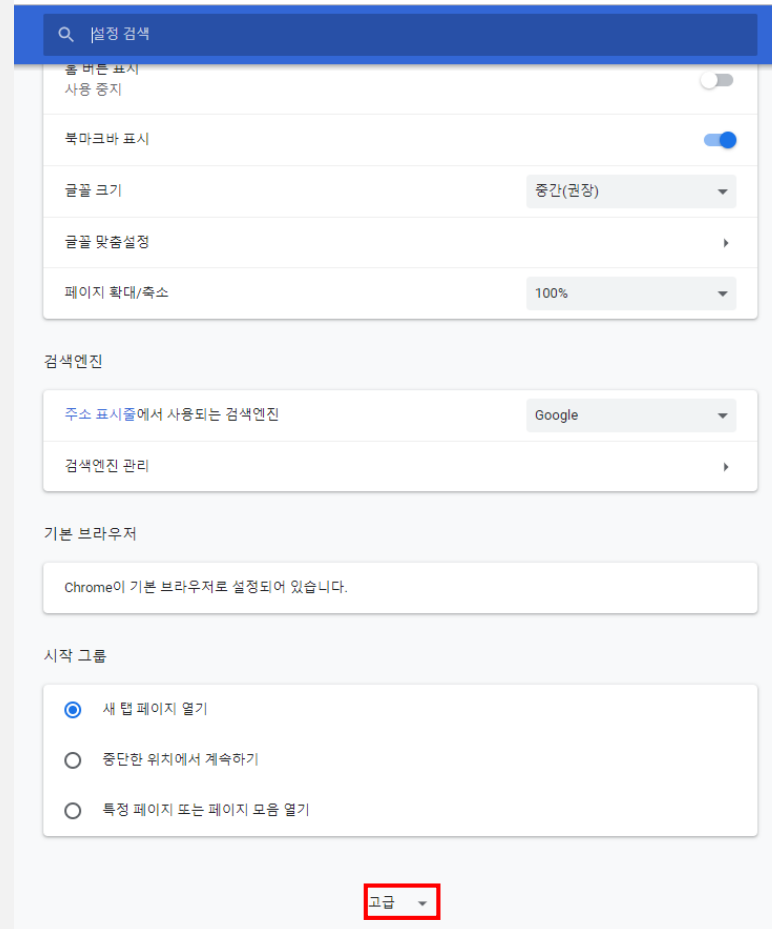
3. Burp Suite Proxy 설정



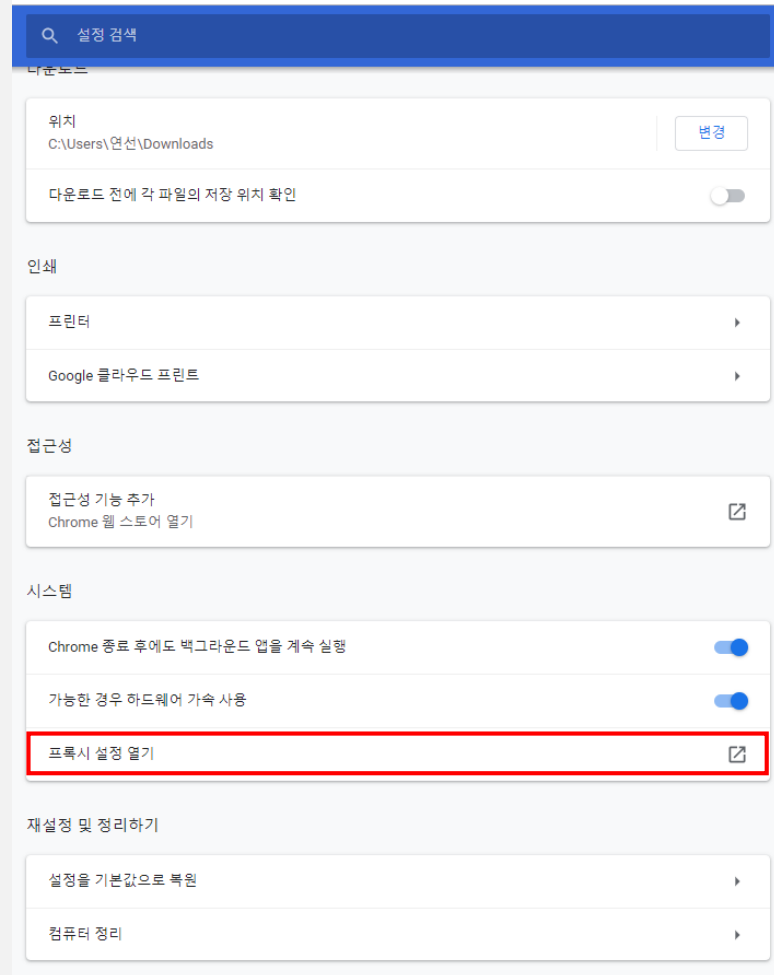
4. Chrome Proxy 설정



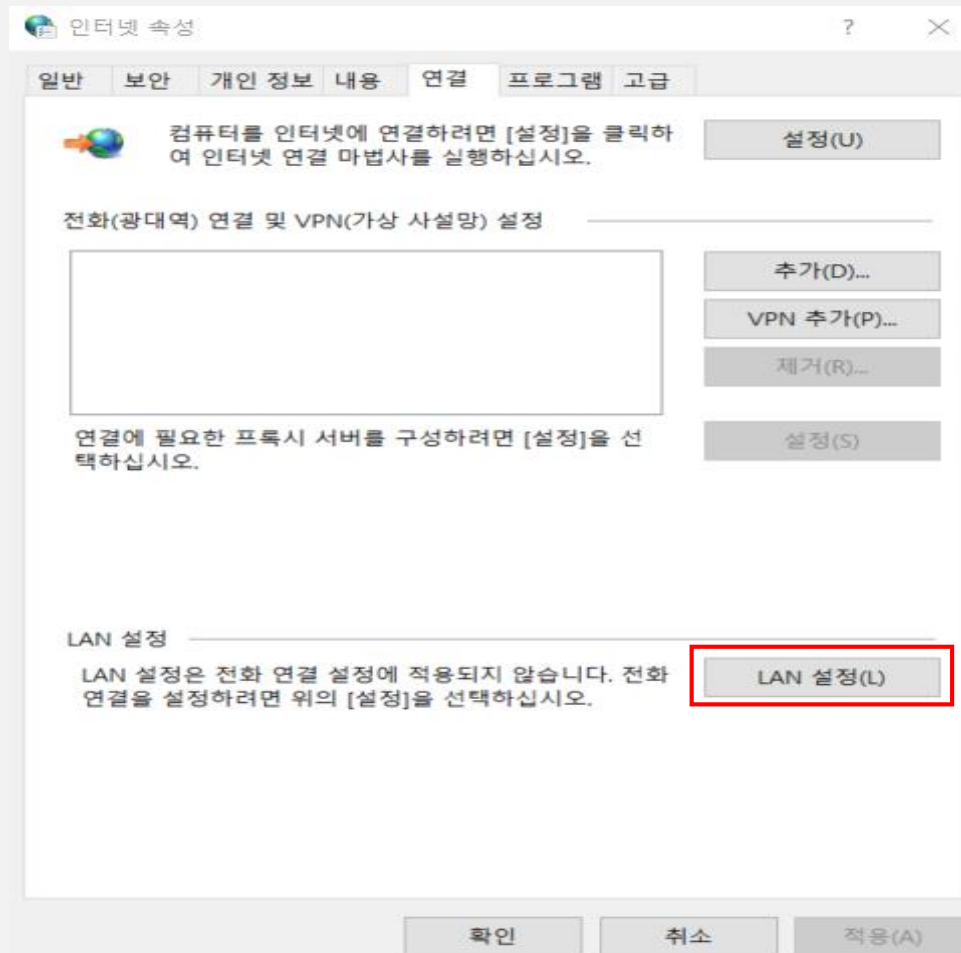
4. Chrome Proxy 설정




4. Chrome Proxy 설정



4. Chrome Proxy 설정



4. Chrome Proxy 설정

 LAN 설정

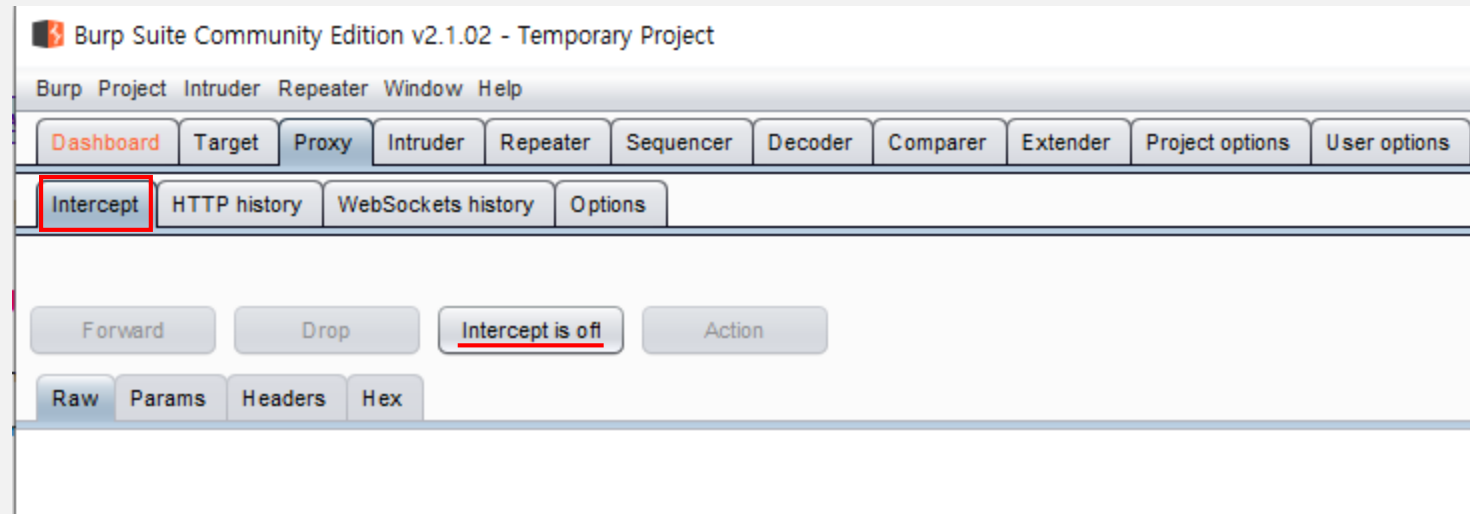
자동 구성
자동 구성은 수동 설정보다 우선합니다. 수동 설정을 사용하려면 자동 구성을 사용하지 마십시오.
☒ 자동으로 설정 검색(A)
☐ 자동 구성 스크립트 사용(S)
주소(R):

프록시 서버
☒ 사용자 LAN에 프록시 서버 사용(이 설정은 전화 연결이나 VPN 연결에는 적용되지 않음)(X)
주소(E): 포트(T): 고급(C)
☐ 로컬 주소에 프록시 서버 사용 안 함(B)

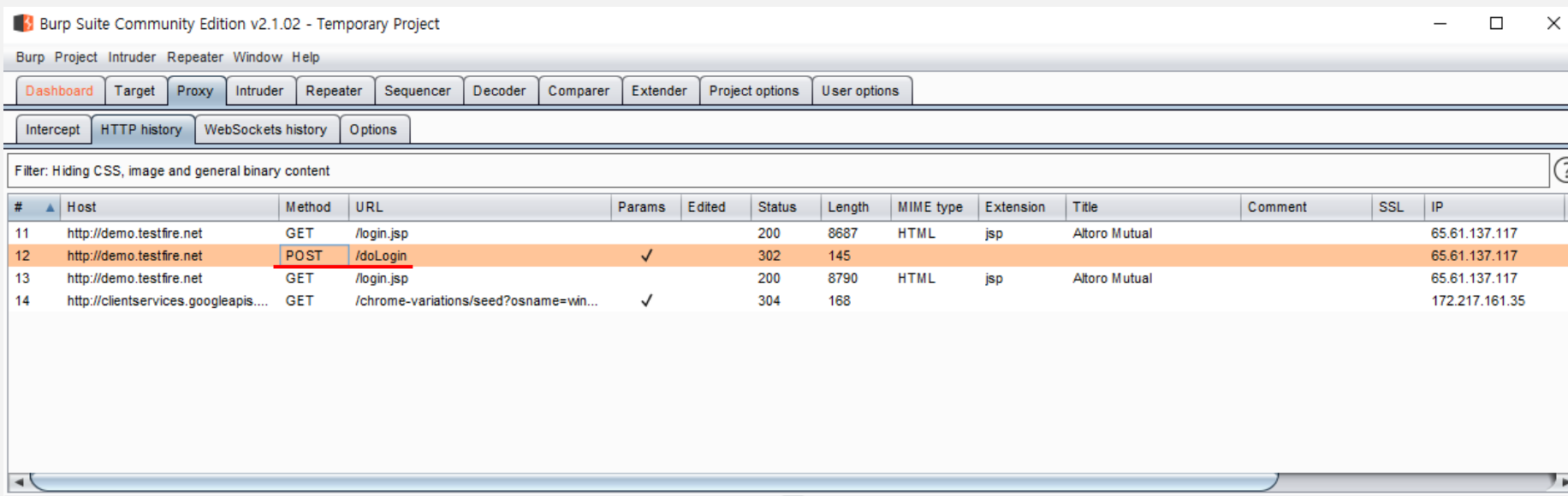
확인

취소

5. HTTP history로 Method 확인



5. HTTP history로 Method 확인



The screenshot shows the Burp Suite Community Edition v2.1.02 interface. The 'HTTP history' tab is selected, displaying a list of intercepted HTTP requests. The second request, a POST to /doLogin, is highlighted in orange. The filter is set to 'Hiding CSS, image and general binary content'.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
11	http://demo.testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.61.137.117
12	http://demo.testfire.net	POST	/doLogin		✓	302	145						65.61.137.117
13	http://demo.testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual			65.61.137.117
14	http://clientservices.googleapis...	GET	/chrome-variations/seed?osname=win...		✓	304	168						172.217.161.35

5. HTTP history로 Method 확인

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
11	http://demo.testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.61.137.117
12	http://demo.testfire.net	POST	/doLogin	✓		302	145						65.61.137.117
13	http://demo.testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual			65.61.137.117
14	http://clientservices.googleapis....	GET	/chrome-variations/seed?osname=win...	✓		304	168						172.217.161.35

Request Response

Raw Params Headers Hex

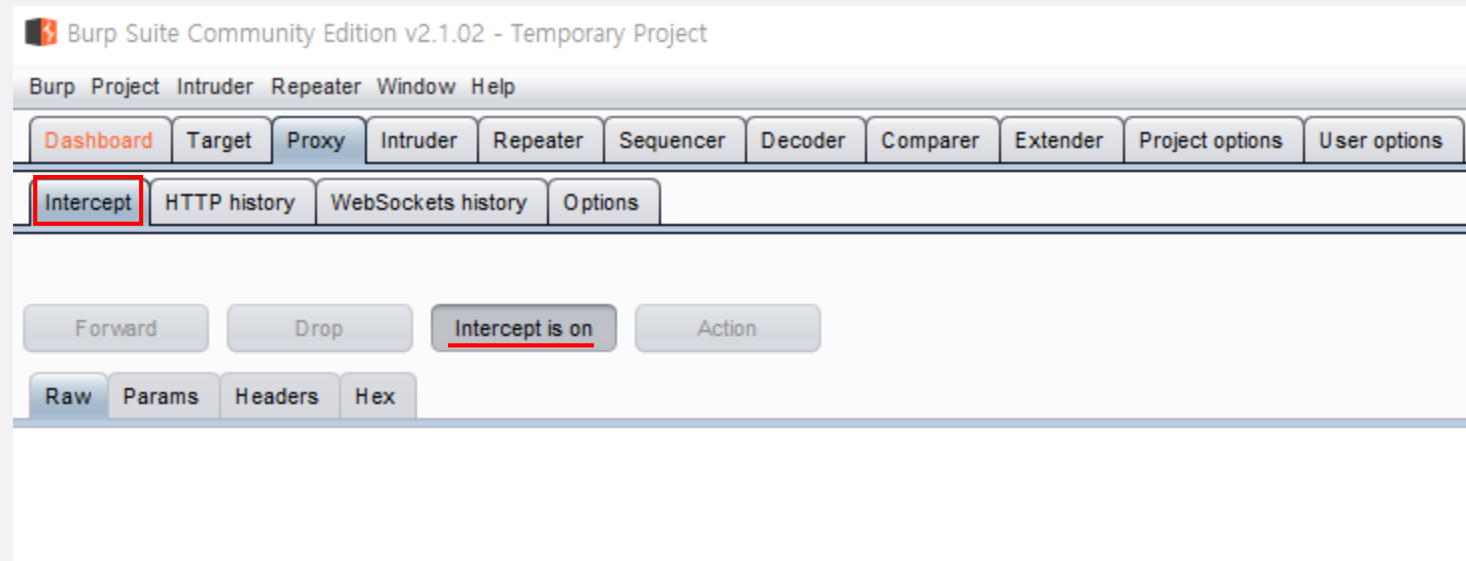
```

POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 36
Cache-Control: max-age=0
Origin: http://demo.testfire.net
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: AltoroAccounts="ODAwMDAwfkNvcnBvcnF0ZX41LjI0MzQ3NzY2M2U3fDgwMDAwMX5DaGVja2luZ341MzgzMC40NHw="; JSESSIONID=1A815EBF20D90B973FC43102838489BE
Connection: close

uid=admin&passw=fd&btnSubmit=Login

```

6. POST Method 수정



6. POST Method 수정

Online Banking Login

Username:	<input type="text" value="admin"/>	ID : admin
Password:	<input type="password" value="*****"/>	Passwd : 1111111
	<input type="button" value="Login"/>	

6. POST Method 수정



Intercept HTTP history WebSockets history Options

Request to http://demo.testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 38
Cache-Control: max-age=0
Origin: http://demo.testfire.net
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: AltoraAccounts="ODAwMDAwfkNvcnBvcnF0ZX41LjI0MzQ3NzY2MUU3fDgwMDAwMX5DaGVja2luZ341MzgzMC40NHw="; JSESSIONID=1A815EBF20D90B973FC43102838489BE
Connection: close

uid=admin&passw=111111&btnSubmit=Login

111111 -> admin으로 수정

6. POST Method 수정



Intercept HTTP history WebSockets history Options

Request to http://demo.testfire.net:80 [65.61.137.117]

Forward Drop Intercept is on Action

Raw Params Headers Hex

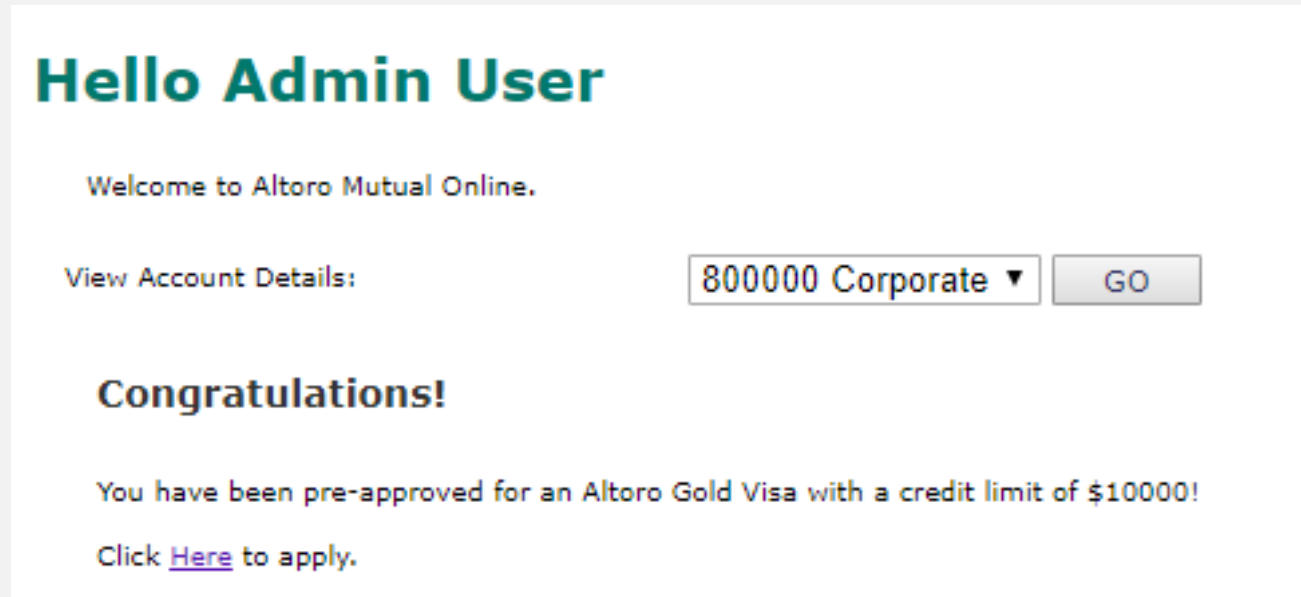
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 37
Cache-Control: max-age=0
Origin: http://demo.testfire.net
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: AltoraAccounts="ODAwMDAwfkNvcnBvcnF0ZX41LjI0MzQ3NzM2MUU3fDgwMDAwMX5DaGVja2luZ341Mzgzc040NHw="; JSESSIONID=1A815EBF20D90B973FC43102838489BE
Connection: close

uid=admin&passw=admin&btnSubmit=Login

111111 -> admin으로 수정

6. POST Method 수정

POST Method 인자를 수정하여
admin 계정 로그인 성공!



The screenshot displays a web interface for 'Altoro Mutual Online'. At the top, it says 'Hello Admin User' in a large, bold, teal font. Below this, a smaller teal text reads 'Welcome to Altoro Mutual Online.' Further down, there is a section titled 'View Account Details:' followed by a dropdown menu showing '800000 Corporate' and a 'GO' button. Below the account details, a bold black text says 'Congratulations!'. Underneath, a teal text states 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!'. At the bottom, a teal text says 'Click [Here](#) to apply.'

Contents 1

GET & POST

https 설정 해제 – chrome://net-internals

Chrome | <chrome://net-internals/#hsts>

Events
Proxy
DNS
Sockets
Domain Security Policy

HSTS/PKP

HSTS is HTTP Strict Transport Security: a way for sites to elect to always use HTTPS. See <https://www.chromium.org/hsts>. PKP is Public Key Pinning: Chrome "pins" certain public keys for certain sites in official builds.

Add HSTS domain

Input a domain name to add it to the HSTS set:

Domain:

Include subdomains for STS: ☐

Query HSTS/PKP domain

Input a domain name to query the current HSTS/PKP set:

Domain:

Expect-CT

Expect-CT allows sites to elect to always require valid Certificate Transparency information. See <https://tools.ietf.org/html/draft-ietf-httpbis-expect-ct>.

Add Expect-CT domain

Input a domain name to add it to the Expect-CT set. Leave Enforce unchecked to configure Expect-CT in report-only mode.

Domain:

Report URI (optional):

Enforce: ☐

Query Expect-CT domain

Input a domain name to query the current Expect-CT set:

Domain:

Send test Expect-CT report

Trigger a test report to the given report URI. The report will contain a hostname of "expect-ct-report.test" and dummy data in other fields.

Report URI:

Delete domain security policies

Input a domain name to delete its dynamic domain security policies (HSTS and Expect-CT). (You cannot delete preloaded entries.):

Domain:

**www.smart.hallym.ac.kr
smart.hallym.ac.kr
입력**

감사합니다