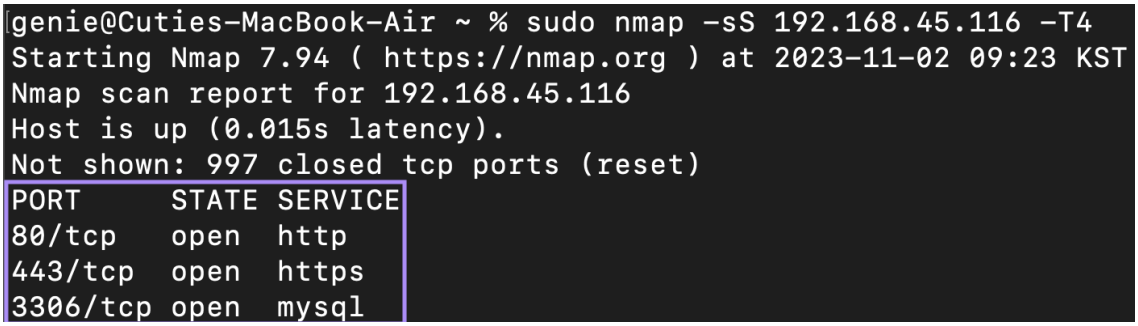
SP_pentest

1. 미흡한 포트 설정으로 인한 데이터베이스 노출

- CVSS 3.1
  - High 8.6
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H
- Endpoint
  - 192.168.45.116
- 취약점 설명
  - 3306 MySQL 포트가 열려있어 해당 포트로 데이터베이스 탈취 가능

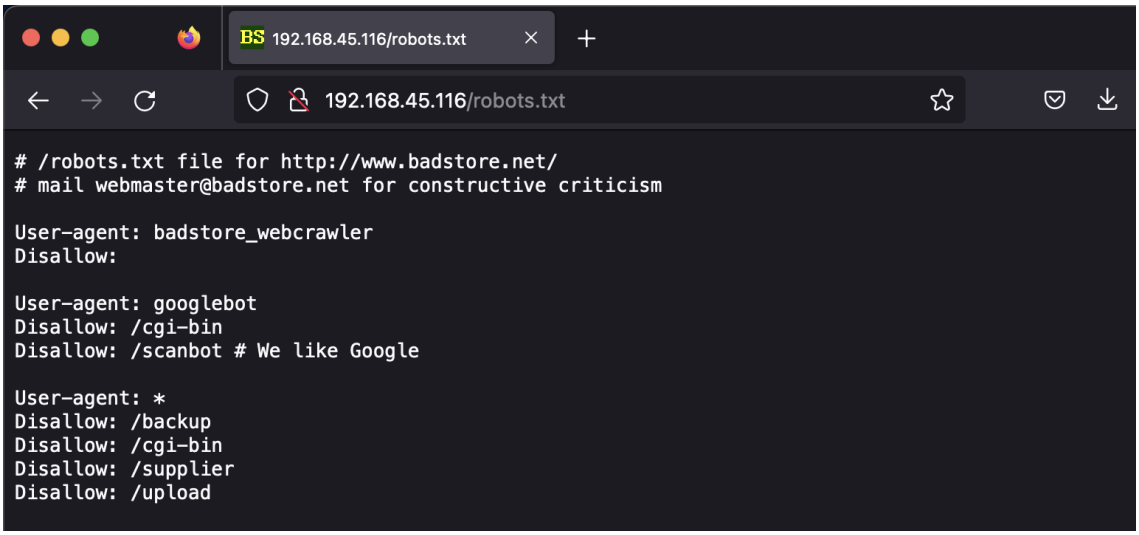


- 취약점 영향
  - 공격자가 해당 포트로 데이터베이스에 접근해 사용자 정보 탈취 가능
  - 관리자 계정 탈취해 사이트 장악 가능
- 조치 방법
  - 3306 포트 닫기
- 취약점 확인 방법
  - nmap scannning

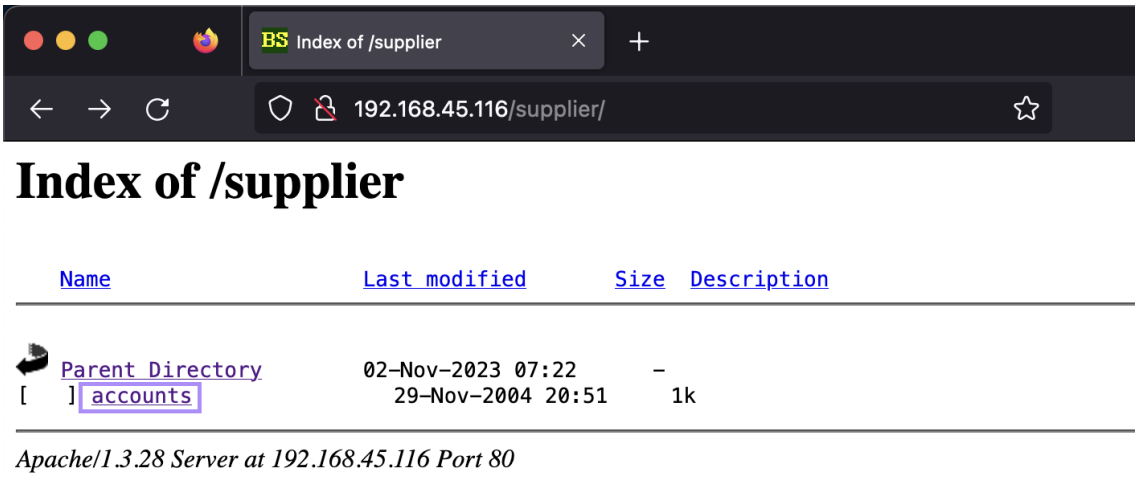
```
sudo nmap -sS 192.168.45.116 -T4
```

2. 엔드포인트 노출로 인한 숨겨진 경로 확인

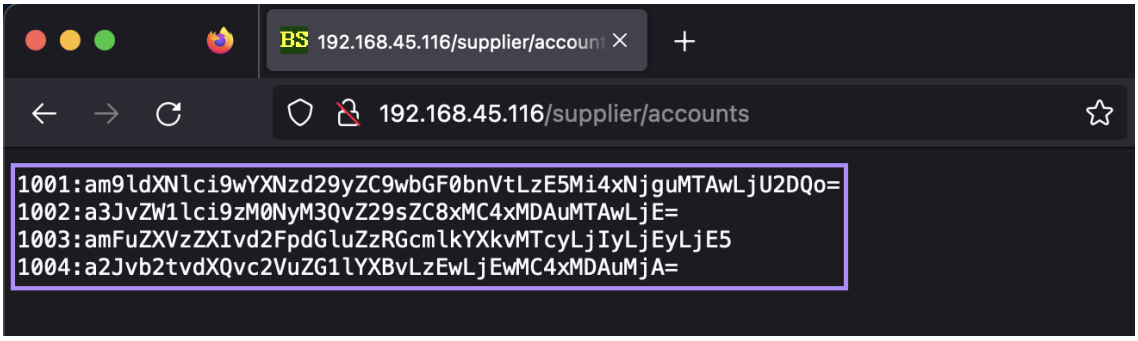
- CVSS 3.1
  - High 7.3
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
- Endpoint
  - 192.168.45.116/robots.txt
- 취약점 설명
  - 검색 엔진에 의해 각종 정보가 검색돼 중요 정보가 노출됨



- 취약점 영향
  - 서플라이어 어카운트 노출됨

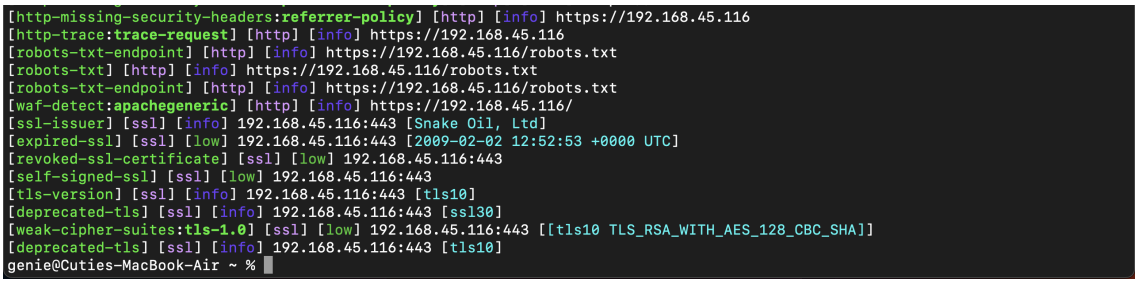


- 마지막 수정 정보 노출됨



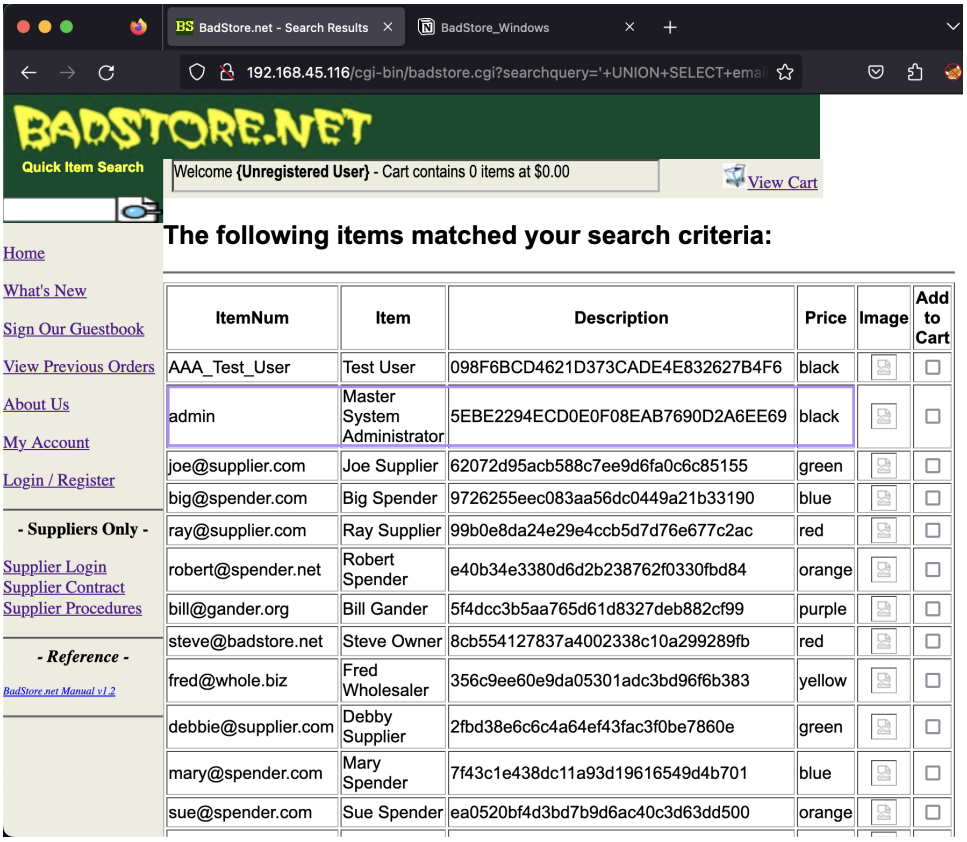
- 조치 방법
  - 모든 검색 로봇(*)에 대해 웹 사이트 전체(/)에 대한 크롤링 차단
  - 검색 엔진으로부터 정보 유출 차단
  - 엔드포인트 암호화
- 취약점 확인 방법
  - Nuclei scanning

```
nuclei -u "192.168.45.116"
```

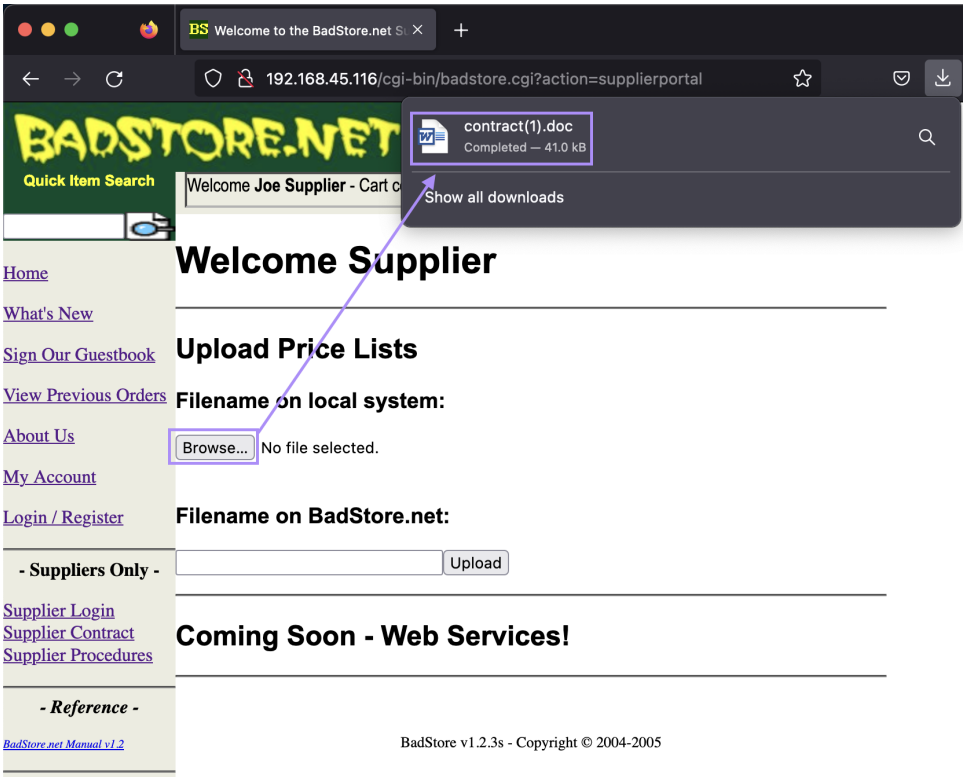


3. SQLi 공격에 의한 데이터베이스 노출

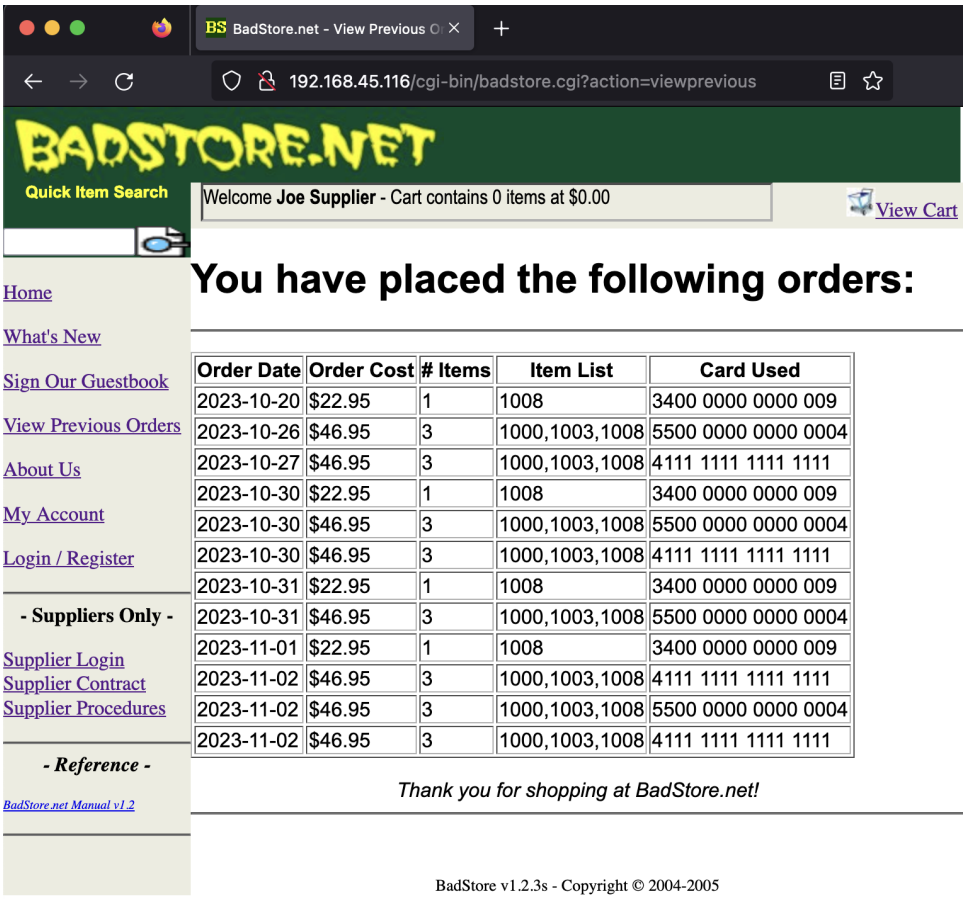
- CVSS 3.1
  - High 9.8
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Endpoint
  - 192.168.45.116/cgi-bin
- 취약점 설명
  - SQLi 공격으로 DB 추출, 사용자 계정정보 추출 가능
- 취약점 영향
  - 어드민 계정 탈취로 서버 장악 및 기밀 접근 가능



- 탈취한 계정으로 기밀 접근 가능



- 사용자 카드 번호 유출



- 조치 방법
  - 입력 값 검증으로 의도하지 않은 입력 값에 대해 검증 및 차단
    - 필터링 대상

> /* - ‘ “ ? # ( ) ; = * +
> UNION, SELECT, DROP, UPDATE, FROM, WHERE, JOIN, SUBSTR
> user_tables, user_table_columns, information_schema, sysobject, table_schema, declare, dual, …

- 취약점 확인 방법
  - 페이지 소스코드로 컬럼명 찾기

```
<HTML><HEAD><TITLE>BadStore.net - Register/Login</TITLE></
<BODY><H2>Login to Your Account or Register for a New Acc
<H3>Login to Your Account</H3>
<FORM METHOD="POST" ACTION="/cgi-bin/badstore.cgi?action=
Email Address:  <INPUT TYPE="text" NAME="email"  SIZE=20 
        <P>Password:  <INPUT TYPE="password" NAME="passwd
        <P><INPUT TYPE="submit" NAME="Login" VALUE="Login
        <FORM METHOD="POST" ACTION="/cgi-bin/badstore.cgi
Full Name:  <INPUT TYPE="text" NAME="fullname"  SIZE=25 MA
        <P>Email Address:  <INPUT TYPE="text" NAME="email
        <P>Password:  <INPUT TYPE="password" NAME="passwd
        <P>Password Hint - What's Your Favorite Color?:  
```

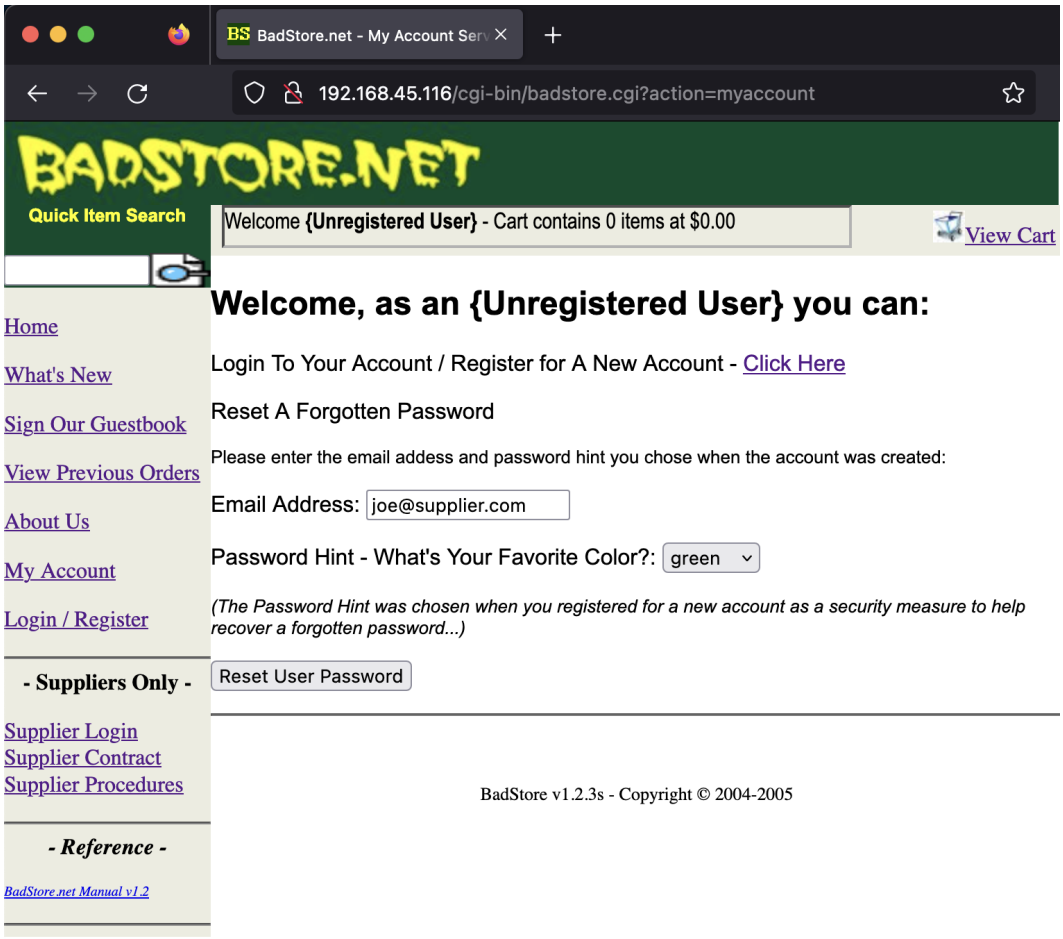
- 이메일, 패스워드, 풀네임, 패스워드 힌트 추출

```
‘UNION SELECT email,fullname,passwd,pwdhint FROM userdb#
```

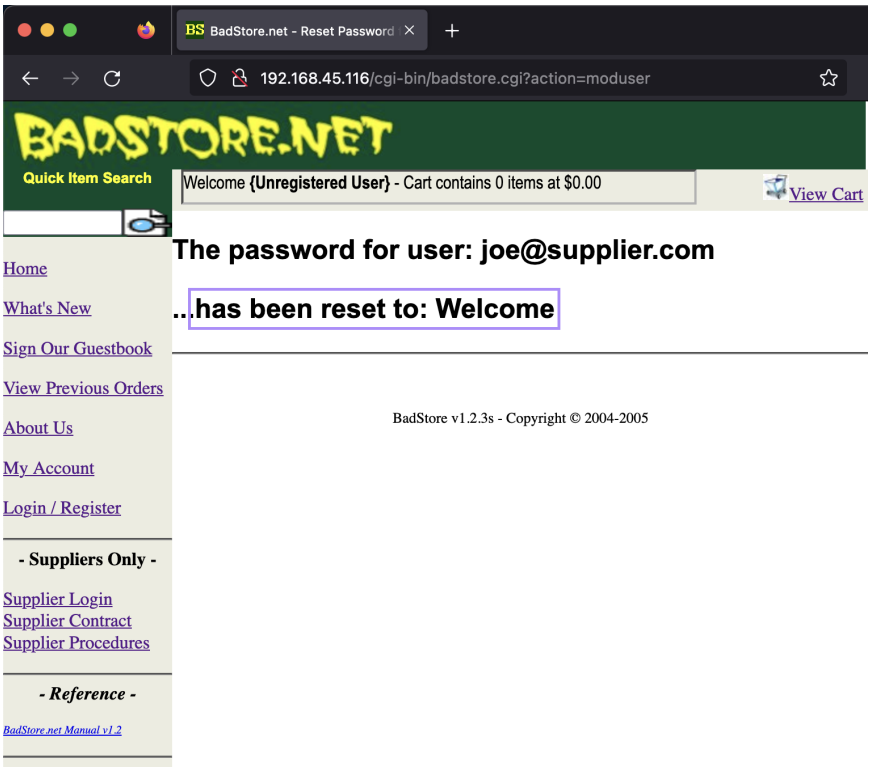
---

4. 미흡한 패스워드 설정과 패스워드 리셋

- CVSS 3.1
  - High 9.8
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Endpoint
  - 192.168.45.116/cgi-bin
- 취약점 설명
  - 패스워드 설정 규칙이 없어서 쉽게 공격 당함
  - 패스워드 변경 인증이 없어서 쉽게 리셋 가능
- 취약점 영향
  - 탈취한 계정 정보로 별다른 인증 절차 없이 쉽게 패스워드 리셋 가능

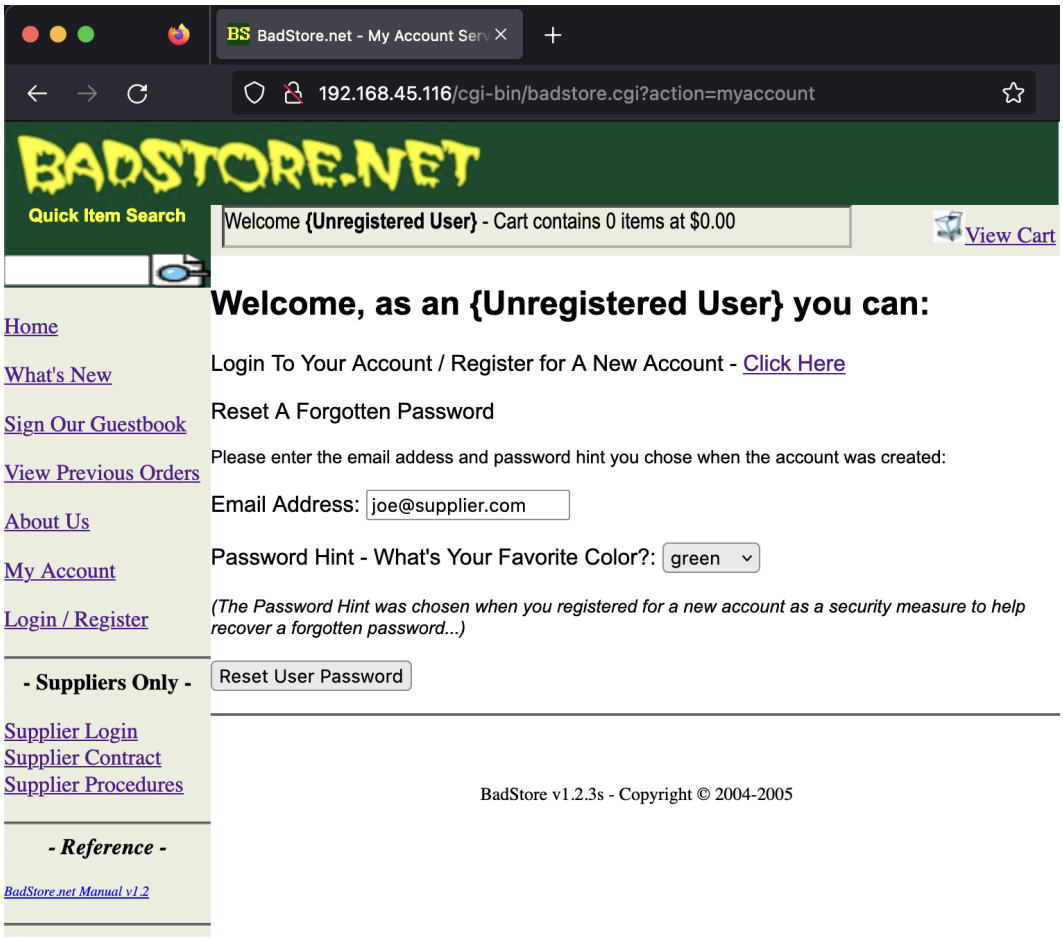


- 리셋된 패스워드는 너무 단순해서 사전공격, 무차별 공격 등에 쉽게 당함



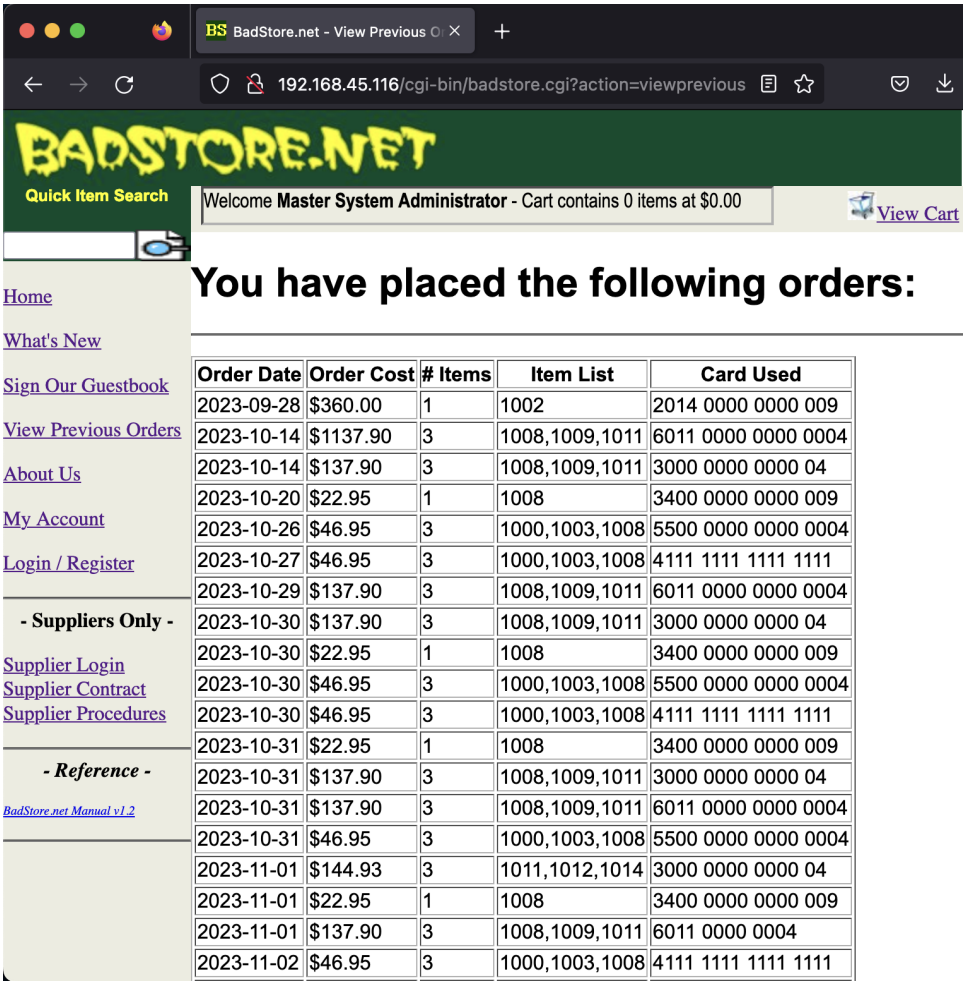
- 조치 방법
  - 영문, 숫자, 특수문자 중 2 종류 이상 조합, 최소 10 자리 이상의 패스워드 설정
  - 영문, 숫자, 특수문자 중 3 종류 이상 조합, 최소 8 자리 이상의 패스워드 설정
  - 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 패스워드 사용 금지
  - 2단계 인증 절차 도입
- 취약점 확인 방법
  - 사용자 계정 리스트를 해킹해 패스워드를 변경함

```
‘UNION SELECT email,fullname,passwd,pwdhint FROM userdb#
```



5. Boolean based SQLi 로 인한 어드민 계정 탈취

- CVSS 3.1
  - High 9.8
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Endpoint
  - 192.168.45.116/cgi-bin/badstore.cgi?action=loginregister
- 취약점 설명
  - 항상 TRUE 값이 되므로 패스워드를 입력하지 않아도 어드민 계정 로그인 가능
- 취약점 영향
  - 어드민 포털 탈취 및 사이트 장악 가능
  - 민감한 데이터에 접근 가능



Order Date	Order Cost	# Items	Item List	Card Used
2023-09-28	$360.00	1	1002	2014 0000 0000 009
2023-10-14	$1137.90	3	1008,1009,1011	6011 0000 0000 0004
2023-10-14	$137.90	3	1008,1009,1011	3000 0000 0000 04
2023-10-20	$22.95	1	1008	3400 0000 0000 009
2023-10-26	$46.95	3	1000,1003,1008	5500 0000 0000 0004
2023-10-27	$46.95	3	1000,1003,1008	4111 1111 1111 1111
2023-10-29	$137.90	3	1008,1009,1011	6011 0000 0000 0004
2023-10-30	$137.90	3	1008,1009,1011	3000 0000 0000 04
2023-10-30	$22.95	1	1008	3400 0000 0000 009
2023-10-30	$46.95	3	1000,1003,1008	5500 0000 0000 0004
2023-10-30	$46.95	3	1000,1003,1008	4111 1111 1111 1111
2023-10-31	$22.95	1	1008	3400 0000 0000 009
2023-10-31	$137.90	3	1008,1009,1011	3000 0000 0000 04
2023-10-31	$137.90	3	1008,1009,1011	6011 0000 0000 0004
2023-10-31	$46.95	3	1000,1003,1008	5500 0000 0000 0004
2023-11-01	$144.93	3	1011,1012,1014	3000 0000 0000 04
2023-11-01	$22.95	1	1008	3400 0000 0000 009
2023-11-01	$137.90	3	1008,1009,1011	6011 0000 0004
2023-11-02	$46.95	3	1000,1003,1008	4111 1111 1111 1111

- 조치 방법
  - 입력 값 검증으로 의도하지 않은 입력 값에 대해 검증 및 차단
    - 필터링 대상

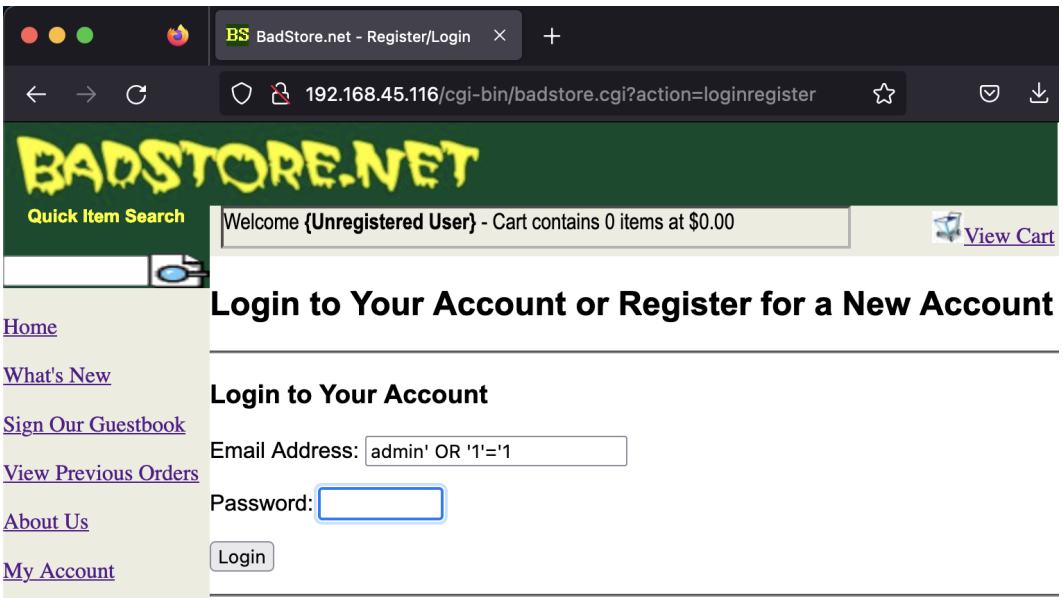
> /* - ‘ “ ? # ( ) ; = * +
> UNION, SELECT, DROP, UPDATE, FROM, WHERE, JOIN, SUBSTR
> user_tables, user_table_columns, information_schema, sysobject, table_schema, declare, dual, …

  - 권장 코드

```
import java.util.regex.Matcher;
import java.util.regex.Pattern;
/* 특수문자 공백 처리*/
final Pattern SpecialCahrs = Pattern.compile("

['\"\\=#()@;=*/+]");
UserInput = SpecialChars.matcher(UserInput).replaceALL("" 

final String regex = "(UNION|SELECT|FROM|WHERE)";

final Pattern pattern = Pattern.compile(regex, Pattern.CAS
final Matcher matcher = Pattern.matcher(UserInput);

if(matcher.find()){
    output.println("<script>alert('No SQL-Injection');</sc
}
```

- 취약점 확인 방법

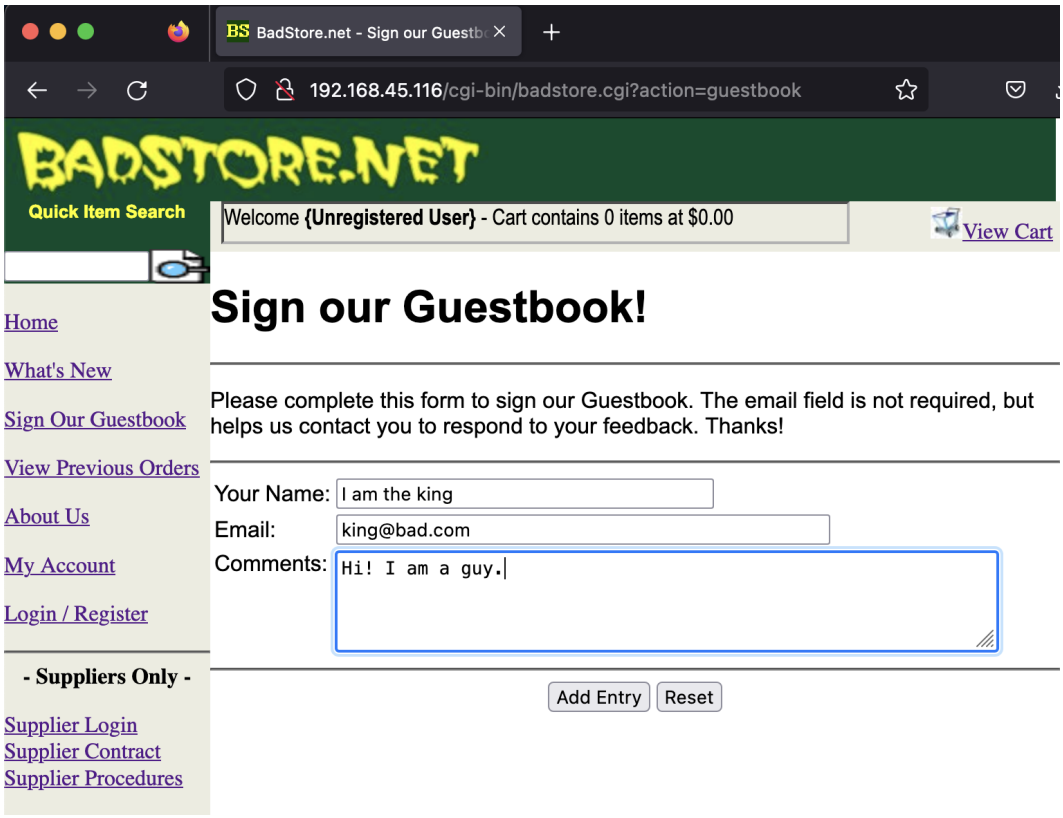
```
admin' OR '1'='1
```

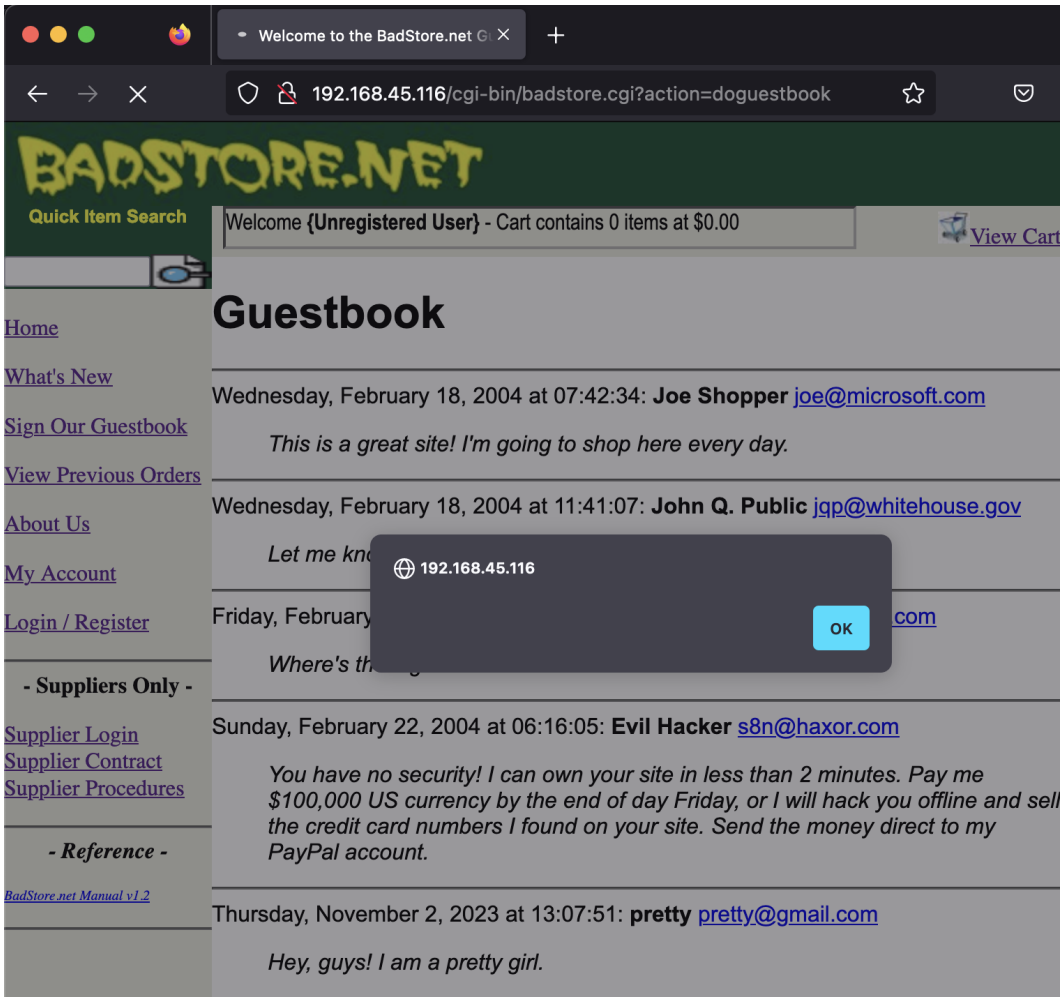


6. XSS 공격으로 인한 사용자 정보 탈취

- CVSS 3.1
  - High 9.8
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Endpoint
  - 192.168.45.116/cgi-bin
- 취약점 설명
  - 악성 URL을 생성 후 조작된 URL을 사용자에게 전송해 사용자가 해당 URL을 클릭하면 정보를 탈취함
  - 웹 서버에 악성 스크립트를 심어놓고 사용자가 방문하면 해당 스크립트를 전달해 사용자의 브라우저를 공격함
- 취약점 영향

- 쿠키 정보, 세션 아이디 등 탈취해 사용자가 수행 가능한 모든 작업을 수행하고 사용자의 데이터에 액세스 가능
- 악성 스크립트가 있는 URL을 클릭하도록 유도해 악성코드나 프로그램이 다운되도록 함





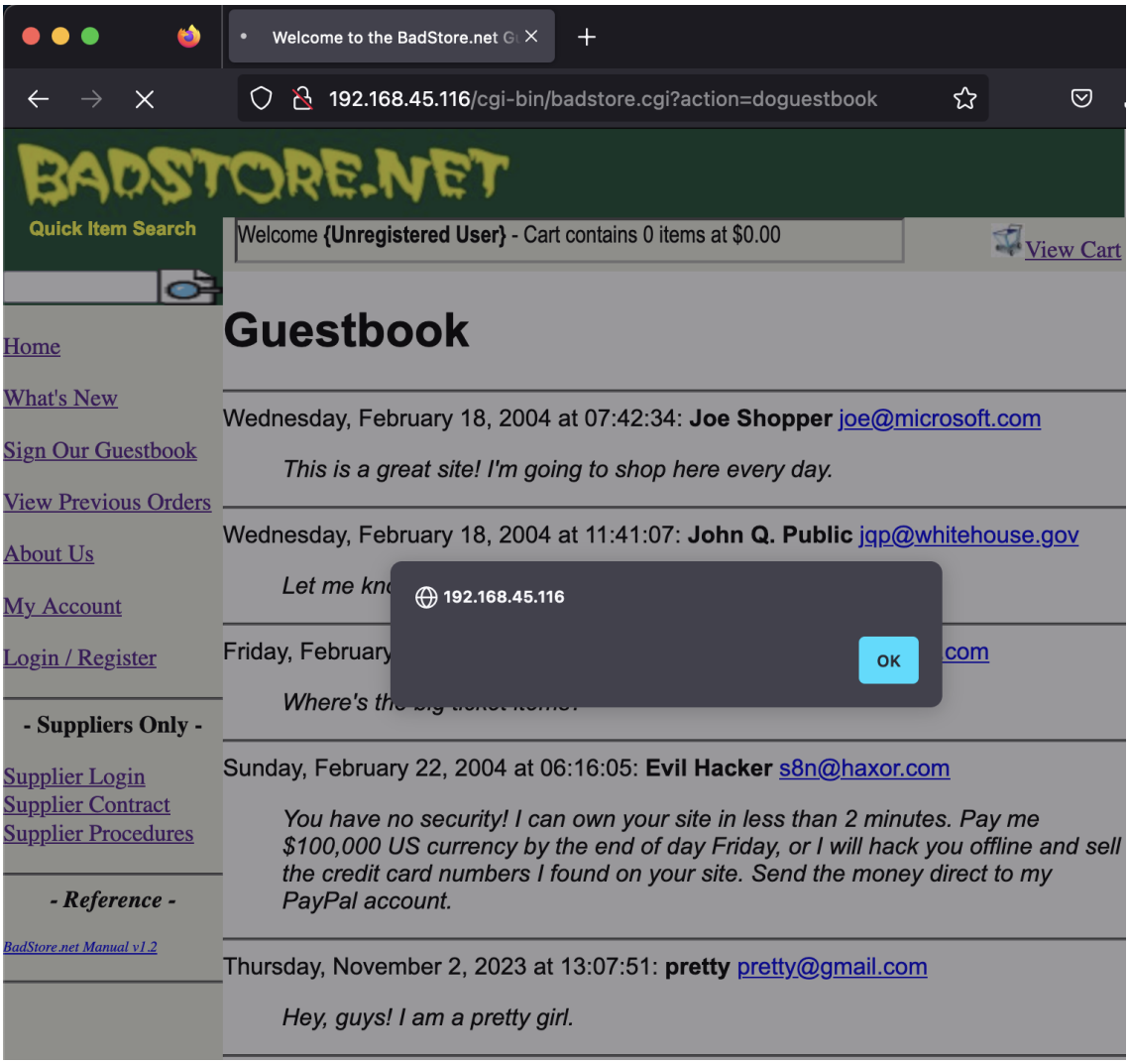
- 조치 방법
  - 입력 값 검증
    - 데이터가 입력되기 전, 입력된 데이터를 서버에 전달하기 전에 프론트에서 검증
    - 입력 데이터의 길이 제한
    - 한글, 영어, 숫자, 공백만 입력 가능하도록 클라이언트 입력 제한 정규식 사용
    - 지정된 문자 또는 형식으로 입력되었는지 확인
    - 정해진 규칙을 벗어난 입력 값들은 무효화
  - 출력 값 검증
    - 스크립트로 해석될 수 있는 특수문자 인코딩

ASCII	참조 문자	ASCII	참조 문자

&	&amp;	“	&quot;
<	&lt;	‘	&#x27;
>	&gt;	/	&#x2F
(	&#40;	)	&#41;

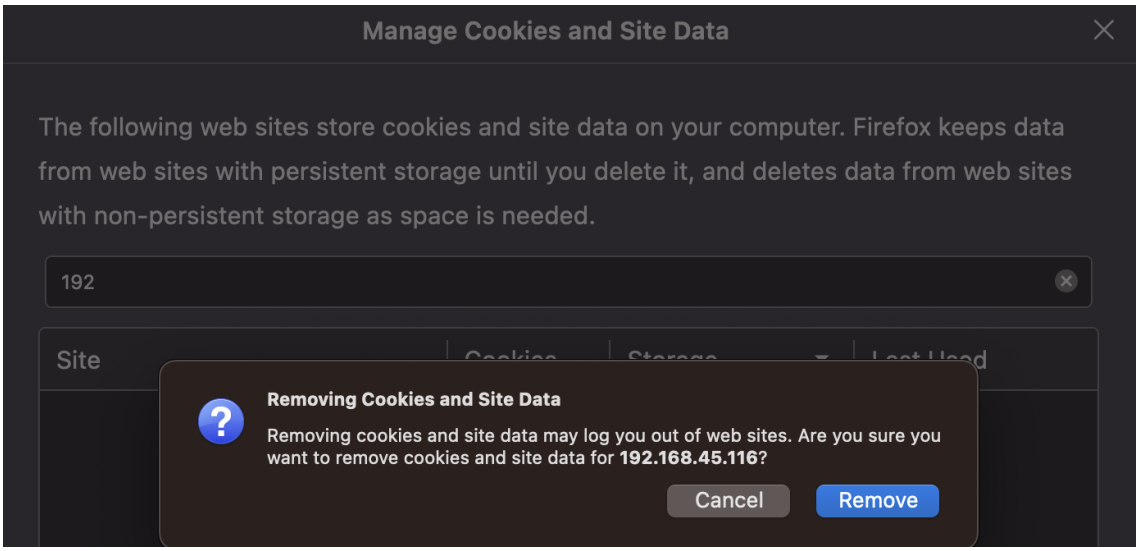
    - 보안 라이브러리 사용
        - AntiXSS Library
        - OWASP Open Source Library
- 취약점 확인 방법
    - Geustbook 에 악성 스크립트 작성

```
<script>alert(document.cookie)</script>
```

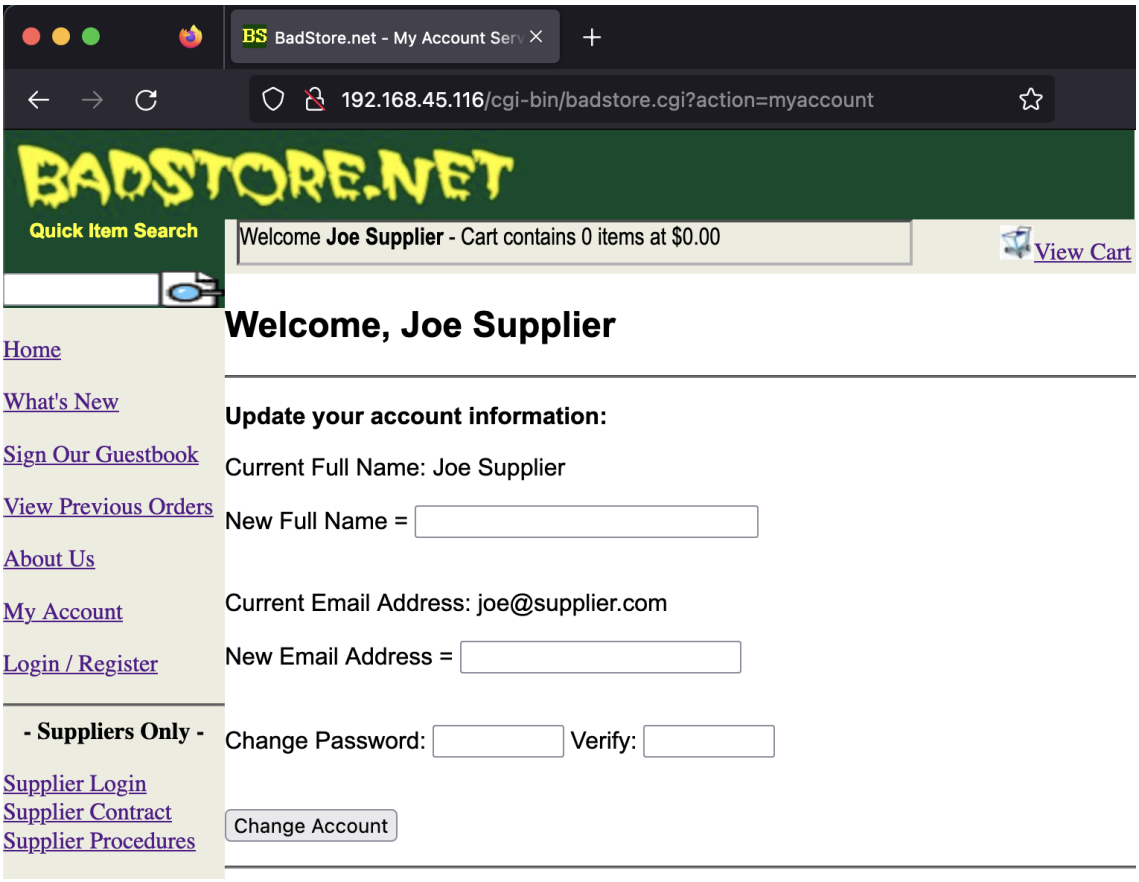


7. 불충분한 세션 관리 및 로그아웃 취약점

- CVSS 3.1
  - High 9.8
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Endpoint
  - 192.168.45.116/cgi-bin/badstore.cgi?action=myaccount
- 취약점 설명
  - 그 어느 곳에도 로그아웃 버튼이 없어 로그아웃 할 수 없음
  - 로그아웃을 위해 쿠키를 삭제해야 함

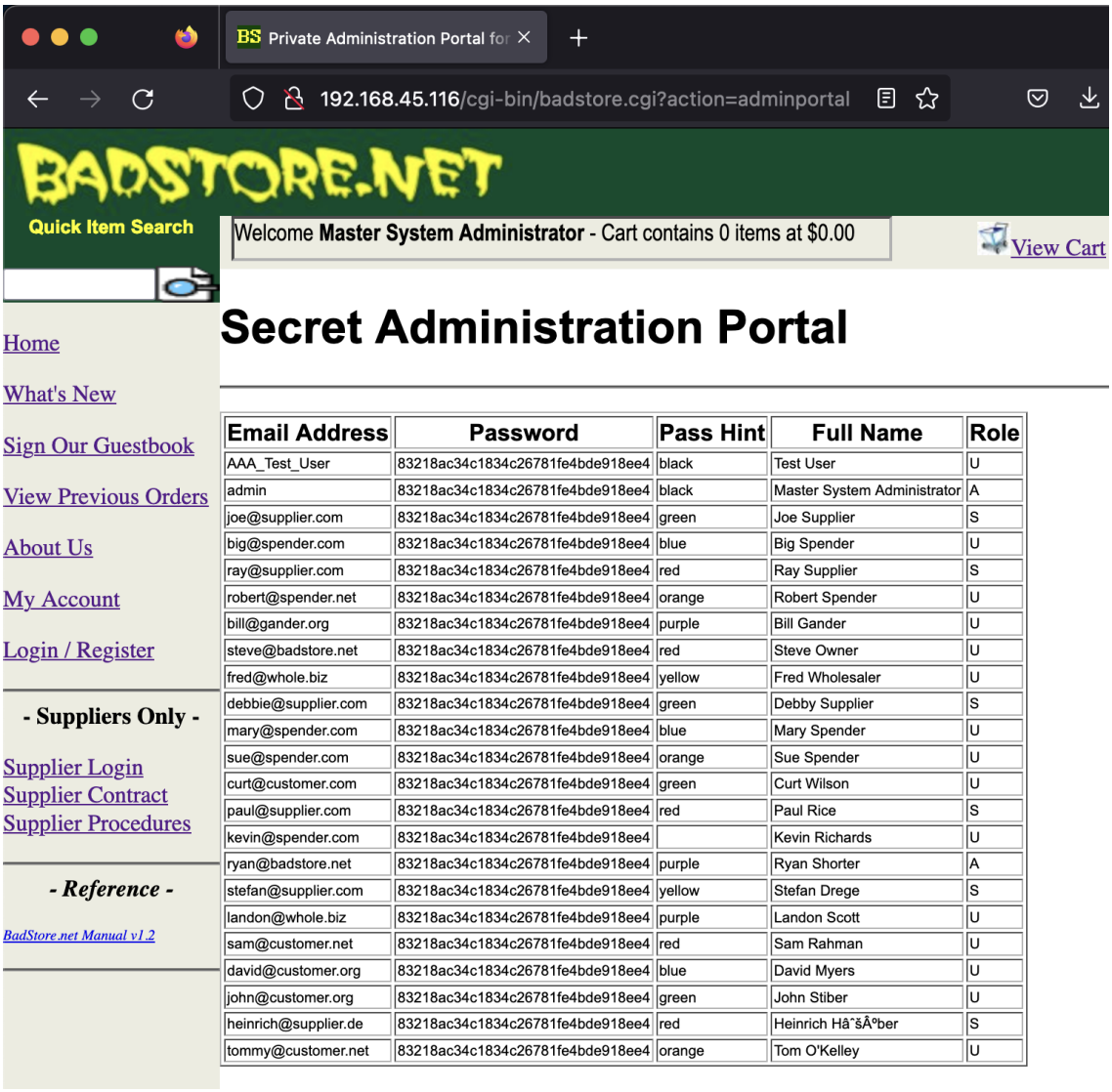


- 취약점 영향
  - 세션 만료 시간이 없어서 로그인이 지속돼 공격자에 의해 세션 탈취 가능
  - 세션 값 변조해 다중 로그인 가능
- 조치 방법
  - 세션 타임아웃 설정으로 20분 이상 아무런 요청이 없을 시 자동 로그아웃
- 취약점 확인 방법
  - 로그아웃 버튼 없음

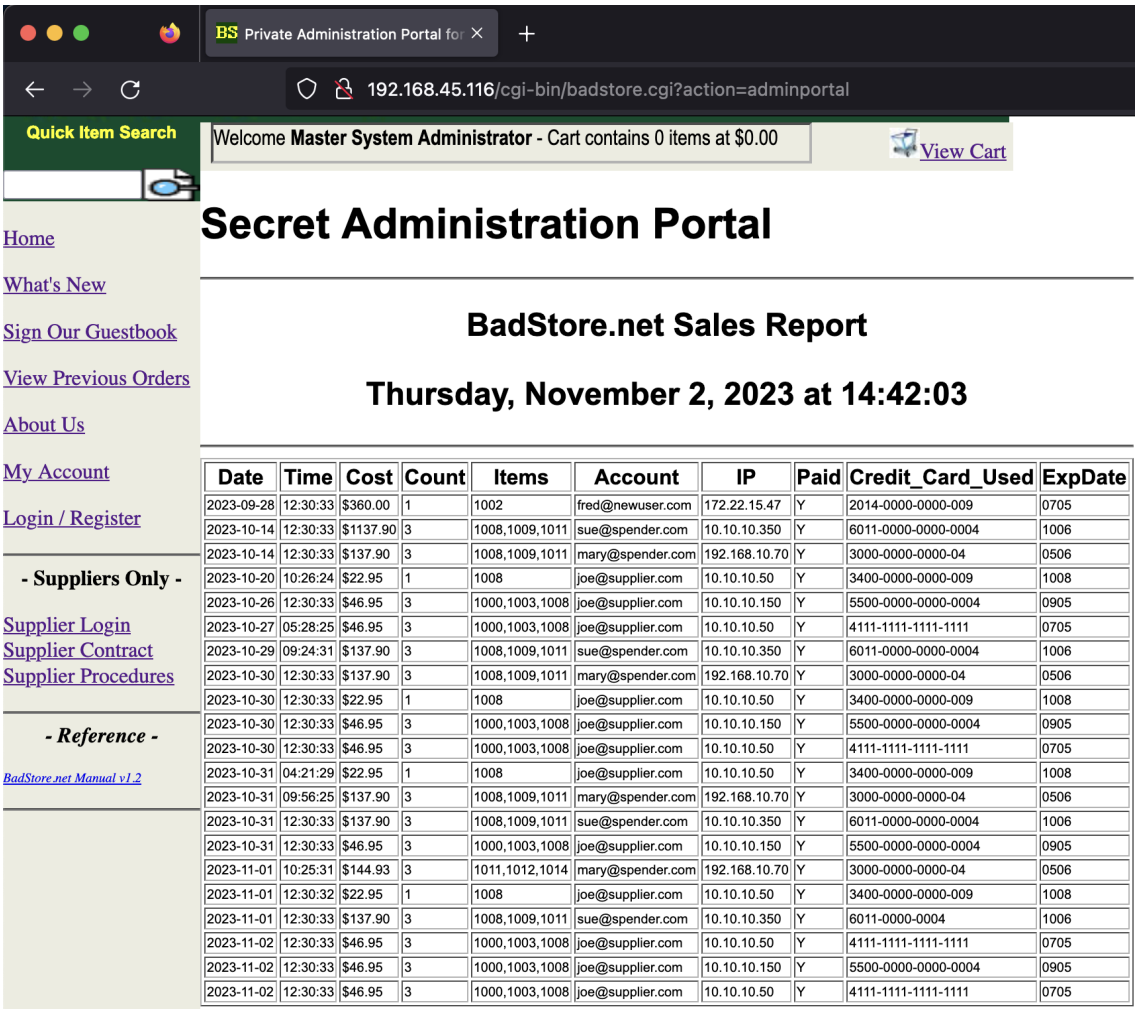


8. 어드민 포털 탈취

- CVSS 3.1
  - High 9.8
  - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Endpoint
  - 192.168.45.116/cgi-bin/badstore.cgi?action=adminportal
- 취약점 설명
  - 적절한 인증 없이 어드민 포털에 접근해 관리 기능과 민감정보 탈취 가능
- 취약점 영향
  - 모든 유저의 정보 탈취

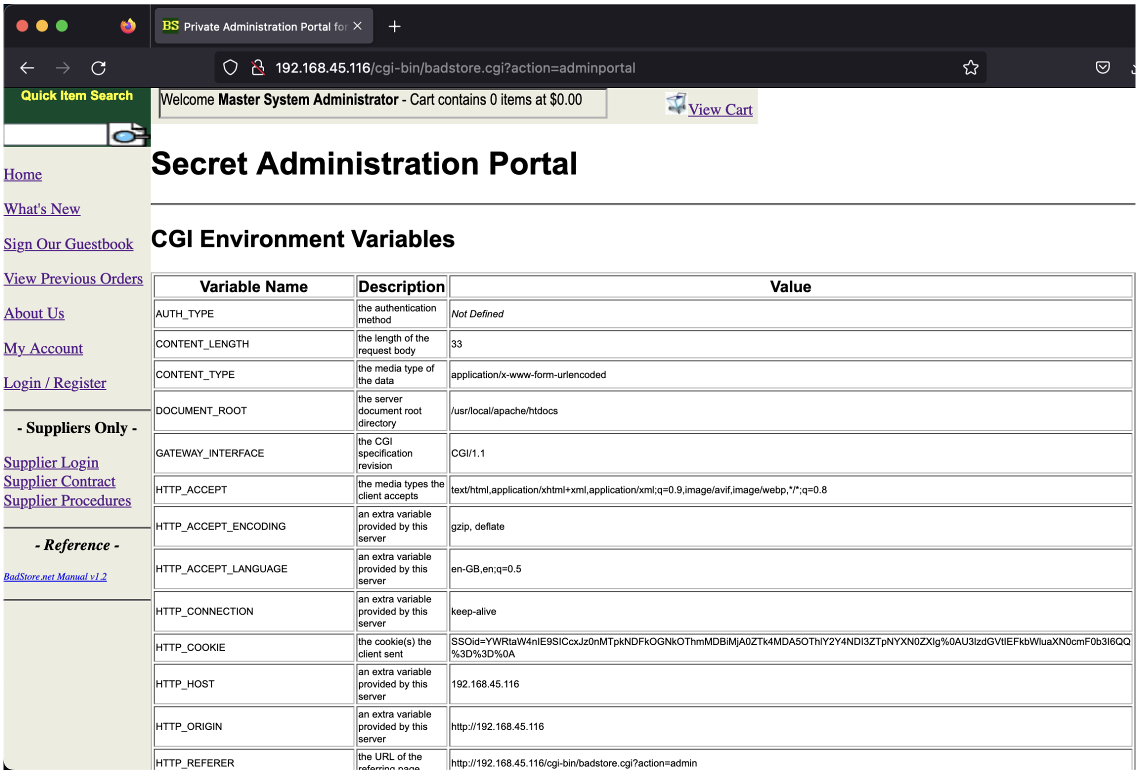


- 세일즈 리포트 등 민감정보 열람



Date	Time	Cost	Count	Items	Account	IP	Paid	Credit_Card_Used	ExpDate
2023-09-28	12:30:33	$360.00	1	1002	fred@newuser.com	172.22.15.47	Y	2014-0000-0000-009	0705
2023-10-14	12:30:33	$1137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2023-10-14	12:30:33	$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-10-20	10:26:24	$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-10-26	12:30:33	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-10-27	05:28:25	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2023-10-29	09:24:31	$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2023-10-30	12:30:33	$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-10-30	12:30:33	$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-10-30	12:30:33	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-10-30	12:30:33	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2023-10-31	04:21:29	$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-10-31	09:56:25	$137.90	3	1008,1009,1011	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-10-31	12:30:33	$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0000-0004	1006
2023-10-31	12:30:33	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-11-01	10:25:31	$144.93	3	1011,1012,1014	mary@spender.com	192.168.10.70	Y	3000-0000-0000-04	0506
2023-11-01	12:30:32	$22.95	1	1008	joe@supplier.com	10.10.10.50	Y	3400-0000-0000-009	1008
2023-11-01	12:30:33	$137.90	3	1008,1009,1011	sue@spender.com	10.10.10.350	Y	6011-0000-0004	1006
2023-11-02	12:30:33	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705
2023-11-02	12:30:33	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.150	Y	5500-0000-0000-0004	0905
2023-11-02	12:30:33	$46.95	3	1000,1003,1008	joe@supplier.com	10.10.10.50	Y	4111-1111-1111-1111	0705

- 최근 아파치 에러 로그, 아파치 액세스 로그에 접근 가능



Quick Item Search

Welcome **Master System Administrator** - Cart contains 0 items at $0.00

View Cart

Home

What's New

Sign Our Guestbook

View Previous Orders

About Us

My Account

Login / Register

- Suppliers Only -

Supplier Login
Supplier Contract
Supplier Procedures

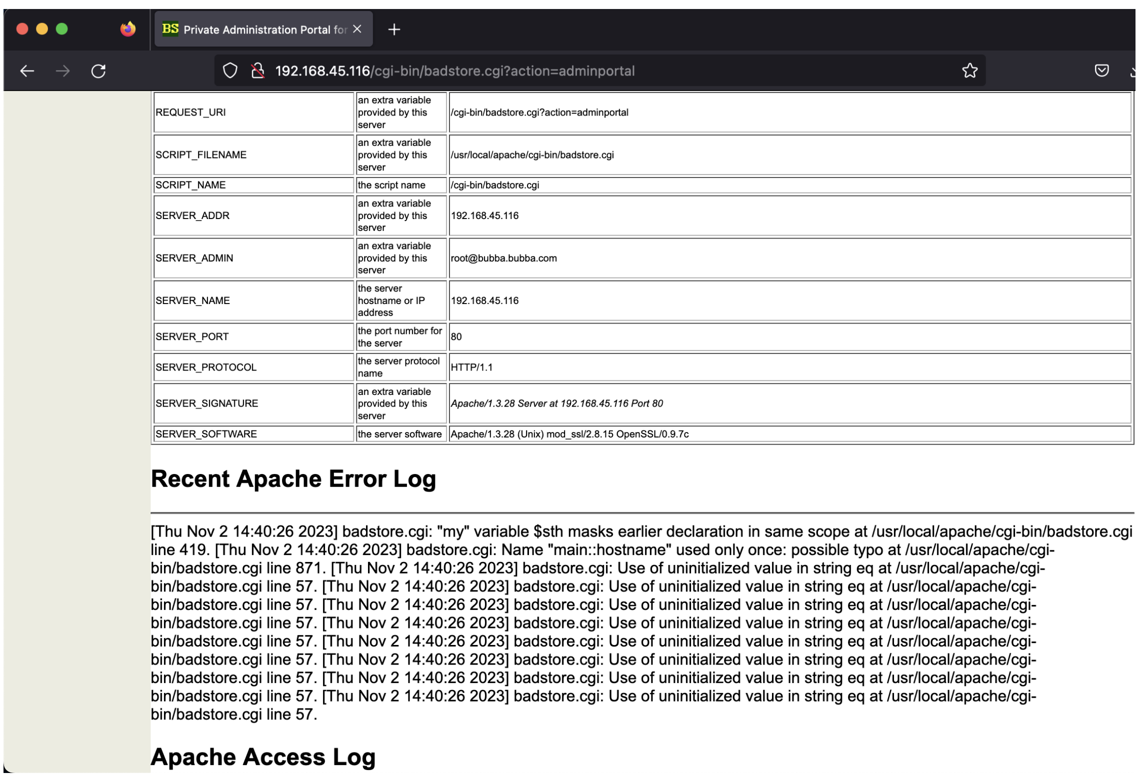
- Reference -

BadStore.net Manual v1.2

Secret Administration Portal

CGI Environment Variables

Variable Name	Description	Value
AUTH_TYPE	the authentication method	*Not Defined*
CONTENT_LENGTH	the length of the request body	33
CONTENT_TYPE	the media type of the data	application/x-www-form-urlencoded
DOCUMENT_ROOT	the server document root directory	/usr/local/apache/htdocs
GATEWAY_INTERFACE	the CGI specification revision	CGI/1.1
HTTP_ACCEPT	the media types the client accepts	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
HTTP_ACCEPT_ENCODING	an extra variable provided by this server	gzip, deflate
HTTP_ACCEPT_LANGUAGE	an extra variable provided by this server	en-GB,en;q=0.5
HTTP_CONNECTION	an extra variable provided by this server	keep-alive
HTTP_COOKIE	the cookie(s) the client sent	SSOid=YWRtaW4nIE9SICcxJz0nMTpkNDFkOGNkOThmMDBiMjA0ZTk4MDA5OThlY2Y4NDI3ZTpNYXN0ZXIg%0AU3lzdGVtIEFkbWluaXN0cmF0b3I6QQ%3D%3D%0A
HTTP_HOST	an extra variable provided by this server	192.168.45.116
HTTP_ORIGIN	an extra variable provided by this server	http://192.168.45.116
HTTP_REFERER	the URL of the referring page	http://192.168.45.116/cgi-bin/badstore.cgi?action=admin



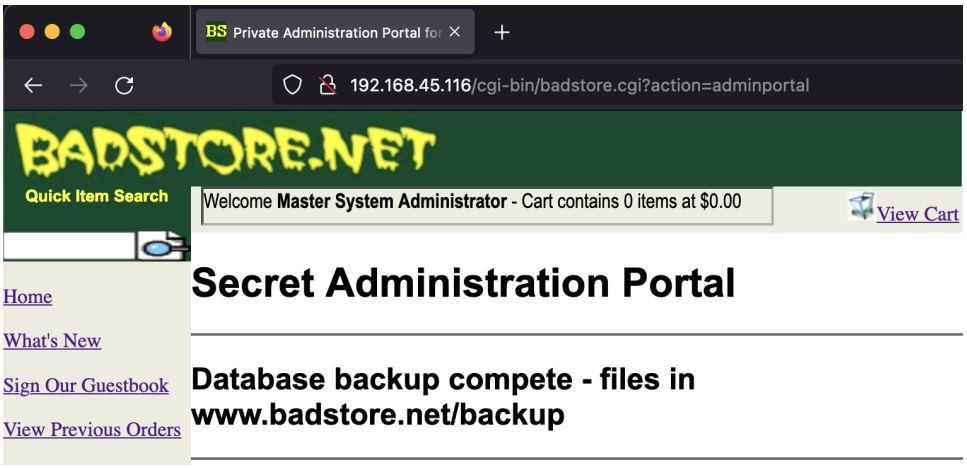
Variable Name	Description	Value
REQUEST_URI	an extra variable provided by this server	/cgi-bin/badstore.cgi?action=adminportal
SCRIPT_FILENAME	an extra variable provided by this server	/usr/local/apache/cgi-bin/badstore.cgi
SCRIPT_NAME	the script name	/cgi-bin/badstore.cgi
SERVER_ADDR	an extra variable provided by this server	192.168.45.116
SERVER_ADMIN	an extra variable provided by this server	root@bubba.bubba.com
SERVER_NAME	the server hostname or IP address	192.168.45.116
SERVER_PORT	the port number for the server	80
SERVER_PROTOCOL	the server protocol name	HTTP/1.1
SERVER_SIGNATURE	an extra variable provided by this server	*Apache/1.3.28 Server at 192.168.45.116 Port 80*
SERVER_SOFTWARE	the server software	Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c

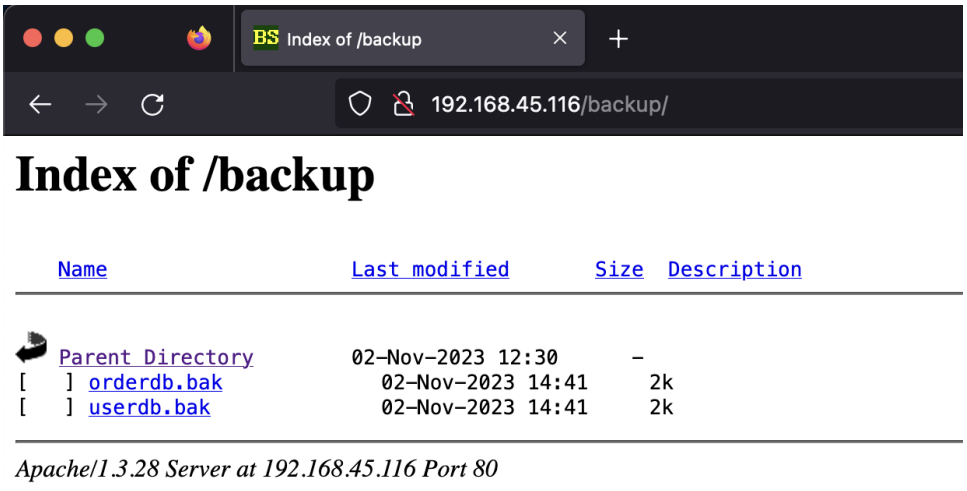
Recent Apache Error Log

[Thu Nov 2 14:40:26 2023] badstore.cgi: "my" variable $sth masks earlier declaration in same scope at /usr/local/apache/cgi-bin/badstore.cgi line 419. [Thu Nov 2 14:40:26 2023] badstore.cgi: Name "main::hostname" used only once: possible typo at /usr/local/apache/cgi-bin/badstore.cgi line 871. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57. [Thu Nov 2 14:40:26 2023] badstore.cgi: Use of uninitialized value in string eq at /usr/local/apache/cgi-bin/badstore.cgi line 57.

Apache Access Log

- 백업 정보 탈취





- 조치 방법
  - 어드민 포털을 쉽게 유추 가능한 URL 사용 금지
  - 외부적으로 특정 IP 범위를 지정해 지정된 사용자만 어디민 포털에 접근할 수 있도록 접근 통제 구축
- 취약점 확인 방법
  - URL로 접근

```
192.168.45.116/cgi-bin/badstore.cgi?action=admin
```

9. SQLi 공격으로 인한 숨겨진 아이템 유출

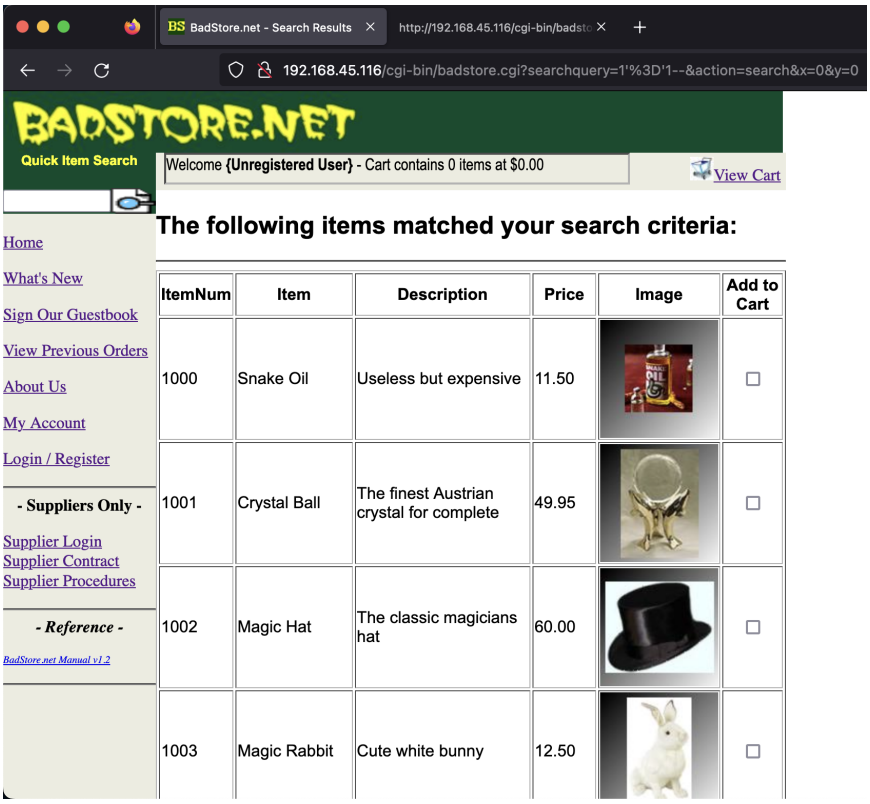
- CVSS 3.1

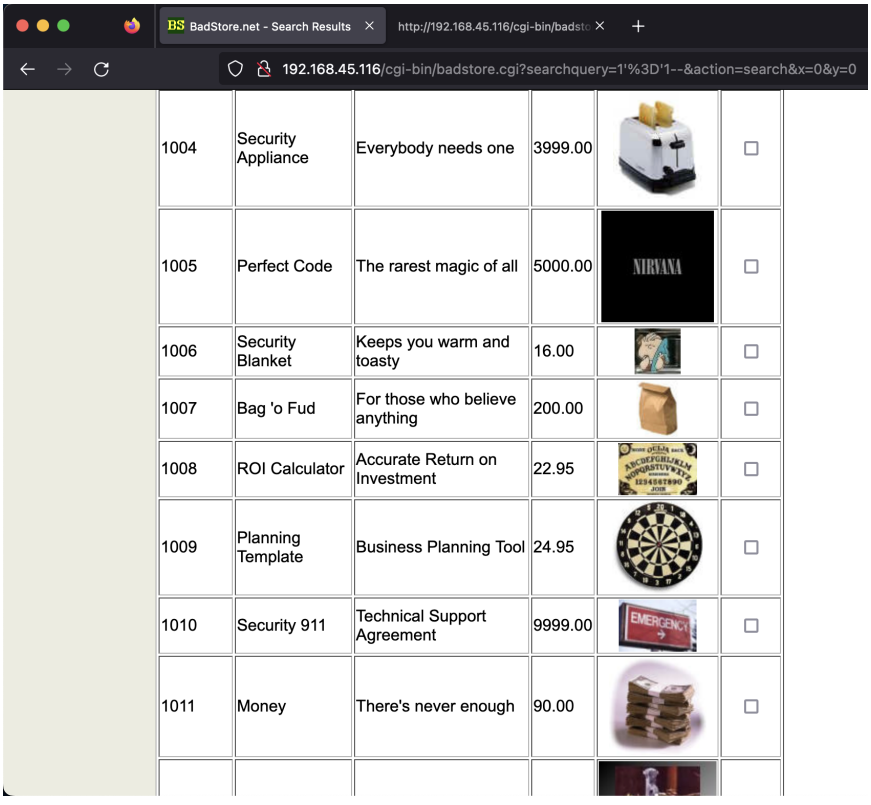
    - High 9.8
    - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Endpoint
    - 192.168.45.116/cgi-bin/badstore.cgi?action=whatsnew
- 취약점 설명
    - 항상 TRUE 값이 되게 해 숨겨진 아이템 유출
- 취약점 영향
    - 숨겨진 아이템 열람으로 기밀 유출 가능
- 조치 방법
    - 입력 값 검증으로 의도하지 않은 입력 값에 대해 검증 및 차단
        - 필터링 대상

> /* - ‘ “ ? # ( ) ; = * +
> UNION, SELECT, DROP, UPDATE, FROM, WHERE, JOIN, SUBSTR
> user_tables, user_table_columns, information_schema, sysobject, table_schema, declare, dual, …

- 취약점 확인 방법
    - What’s New 검색창에 SQLi 공격

```
1'='1--
```


BadStore.net - Search Results
http://192.168.45.116/cgi-bin/badsto
192.168.45.116/cgi-bin/badstore.cgi?searchquery=1'%3D'1--&action=search&x=0&y=0
BADSTORE.NET
Quick Item Search
Welcome {Unregistered User} - Cart contains 0 items at $0.00
View Cart
Home
What's New
Sign Our Guestbook
View Previous Orders
About Us
My Account
Login / Register
- Suppliers Only -
Supplier Login
Supplier Contract
Supplier Procedures
- Reference -
BadStore.net Manual v1.2
The following items matched your search criteria:
ItemNum
Item
Description
Price
Image
Add to Cart
1000
Snake Oil
Useless but expensive
11.50
1001
Crystal Ball
The finest Austrian crystal for complete
49.95
1002
Magic Hat
The classic magicians hat
60.00
1003
Magic Rabbit
Cute white bunny
12.50


BadStore.net - Search Results
http://192.168.45.116/cgi-bin/badsto
192.168.45.116/cgi-bin/badstore.cgi?searchquery=1'%3D'1--&action=search&x=0&y=0
1004
Security Appliance
Everybody needs one
3999.00
1005
Perfect Code
The rarest magic of all
5000.00
NIRVANA
1006
Security Blanket
Keeps you warm and toasty
16.00
1007
Bag 'o Fud
For those who believe anything
200.00
1008
ROI Calculator
Accurate Return on Investment
22.95
1009
Planning Template
Business Planning Tool
24.95
1010
Security 911
Technical Support Agreement
9999.00
EMERGENCY
1011
Money
There's never enough
90.00

1012	Endless Cup	Perfect for late nights	23.98		☐
1013	Invisibility Cloak	For when you just want to hide	8995.00		☐
1014	Disappearing Ink	Makes perfect signatures	30.95		☐
9999	Test	Test Item	0.00	TEST	☐

Add Items to Cart Reset