

취약점 진단

1. 취약점 진단의
정의

취약점 진단 이 라?



취약점을 발견하기 위한 테스트 방법



웹 취약점 진단

웹 모의해킹

웹 침투 테스트

취약점 진단

1. 취약점 진단의 정의

웹 취약점 진단

웹 모의해킹

웹 침투테스트

웹 어플리케이션 또는 웹 페이지 등 웹으로 구현되는 시스템에 취약점이 존재하는지 체크

취약점 진단

1. 취약점 진단의 정의

웹 취약점 진단

웹 모의해킹

웹 침투테스트

취약점을 이용해서 실제 정보를 유출하거나, 확인하는 정도까지의 행위

취약점 진단

1. 취약점 진단의 정의

웹 취약점 진단

웹 모의해킹

웹 침투테스트

웹 시스템을 이용하여 실제 시스템으로 침투하기 때문에 모의 해킹과 유사

취약점 진단

2. 취약점 진단 수행 절차

테스트 케이스 작성

취약점 진단 실시

진단 결과 검증

보고서 작성



3. 취약점 진단 도
구

취약점 진단 도 구



자동 진단 도구

수동 진단 보조
도구

취약점 진단

3. 취약점 진단 도구

자동 진단 도구

- 진단 대상을 기록하는 기능
- 시나리오 작성 기능

테스트 케이스
작성 기능

취약점 진단
수행 기능

테스트 케이스 작성 기능에서 만든 테스트
케이스를 바탕으로 웹 페이지의 취약점을
찾아내는 기능

보고서 작성
기능

취약점 진단 수행 기능으로 발견한 취약
점을 정리해 보고서를 만드는 기능

3. 취약점 진단 도구

수동 진단 보조 도구

프록시

웹 서버와 웹 브라우저 사이의 통신에 끼어들어 HTTP 요청 및 응답을 확인하거나 내용 변조

리피터

전송한 요청을 다시 전송하는 반복 요청 기능

퍼저

자동으로 값을 GET 또는 POST 데이터, 헤드 필드와 같은 매개 변수에 삽입해 요청을 보내는 기능

3. 취약점 진단 도구

수동 진단 보조 도구

인코더

지정한 문자열을 Base64나 URL 인코드
등으로 인코딩하거나 디코딩하는 기능

diff

2개의 로그를 비교해 변경 내용을 찾아내
는 기능

기타 진단 보
조 기능

- 토큰 관리 기능
- Replace 기능

3. 취약점 진단 도구

수동 진단 보조 도구

인코더

지정한 문자열을 Base64나 URL 인코드
등으로 인코딩하거나 디코딩하는 기능

diff

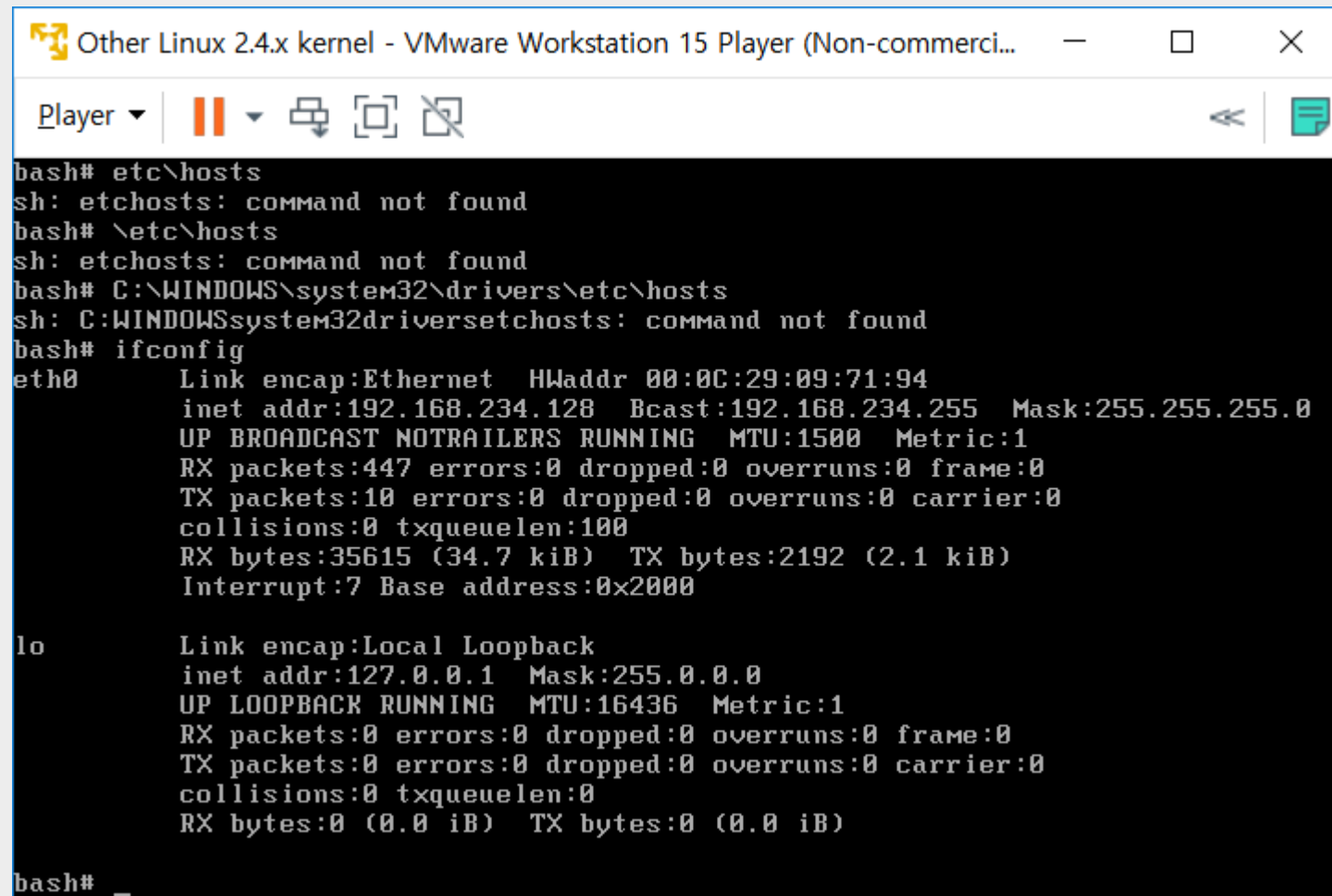
2개의 로그를 비교해 변경 내용을 찾아내
는 기능

기타 진단 보
조 기능

- 토큰 관리 기능
- Replace 기능

취약점 진단

4. 자동 진단 도구 실습



```
Other Linux 2.4.x kernel - VMware Workstation 15 Player (Non-commercial)
Player
bash# etc\hosts
sh: etchosts: command not found
bash# \etc\hosts
sh: etchosts: command not found
bash# C:\WINDOWS\system32\drivers\etc\hosts
sh: C:WINDOWSsystem32driversetchosts: command not found
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:09:71:94
          inet addr:192.168.234.128  Bcast:192.168.234.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:447 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:35615 (34.7 kiB)  TX bytes:2192 (2.1 kiB)
          Interrupt:7 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 iB)  TX bytes:0 (0.0 iB)

bash# _
```

취약점 진단

4. 자동 진단 도구 실습



취약점 진단

4. 자동 진단 도구 실습

Untitled Session - OWASP ZAP 2.7.0

파일 Edit View Analyse 보고서 Tools Online Help

Standard Mode

Sites +

Header: Text Body: Text

Contexts

- Default Context
- Sites
 - https://incoming.telemetry.mozilla.org
 - http://192.168.234.128
 - cgi-bin
 - DoingBusiness
 - GET:favicon.ico
 - GET:frmvrty.js
 - images
 - Procedures
 - https://adservice.google.com
 - https://adservice.google.co.kr
 - http://survey.g.doubleclick.net

HTTP/1.1 200 OK
Date: Wed, 19 Dec 2018 22:46:12 GMT
Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Last-Modified: Sun, 14 May 2006 21:16:23 GMT
ETag: "14b-dff-44679e27"
Accept-Ranges: bytes
Content-Length: 3583
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<HTML><HEAD><TITLE>Welcome to BadStore.net v1.2.3</TITLE></HEAD>
<BODY bgColor=#ffffff leftMargin=0 topMargin=0 MARGINHEIGHT="0" MARGINWIDTH="0">
<TABLE cellSpacing=0 cellPadding=0 width=760 bgColor=#004b2c border=0>
<TBODY>
<TR>
<TD width=326 bgColor=#004b2c>
<IMG height=60 alt="BadStore.net" hspace=0 src="/images/BadStore.jpg"
width=350
border=0>

History Search 경고 Output WebSockets +

필터: OFF Export

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
182	18. 12. 19 오후 10:49:43	GET	http://192.168.234.128/cgi-bin/bsheader.cgi	200	OK	30 ms	136 bytes	Medium		
183	18. 12. 19 오후 10:49:46	GET	http://192.168.234.128/cgi-bin/badstore.cgi	200	OK	27 ms	4,046 bytes	Medium		Form, Hidden
184	18. 12. 19 오후 10:49:46	GET	http://192.168.234.128/cgi-bin/bsheader.cgi	200	OK	25 ms	136 bytes	Medium		
185	18. 12. 19 오후 10:49:51	GET	http://192.168.234.128/cgi-bin/badstore.cgi?action...	200	OK	27 ms	3,982 bytes	Medium		Form, Hidden
186	18. 12. 19 오후 10:49:51	GET	http://192.168.234.128/cgi-bin/bsheader.cgi	200	OK	21 ms	136 bytes	Medium		
187	18. 12. 19 오후 10:49:59	GET	http://192.168.234.128/cgi-bin/badstore.cgi	200	OK	31 ms	4,046 bytes	Medium		Form, Hidden
188	18. 12. 19 오후 10:49:59	GET	http://192.168.234.128/cgi-bin/bsheader.cgi	200	OK	26 ms	136 bytes	Medium		
189	18. 12. 19 오후 10:50:16	GET	http://badstore.com/	302	Found	385 ms	0 bytes			
190	18. 12. 19 오후 10:50:17	GET	http://badstore.com/SpRbZ/	302	Found	381 ms	0 bytes			
191	18. 12. 19 오후 10:50:17	GET	http://badstore.com/	200	OK	466 ms	372 bytes	Medium		Comment
193	18. 12. 19 오후 10:50:21	GET	http://192.168.234.128/	200	OK	3 ms	3,583 bytes	Medium		Form, Hidden

Alerts 0 1 6 0 Current Scans 0 0 0 0 0 0 0 0

취약점 진단

4. 자동 진단 도구 실습

Untitled Session - OWASP ZAP 2.7.0

파일 Edit View Analyse 보고서 Tools Online Help

Standard Mode

Sites + 빠른 시작 Request Response +

Contexts

- Default Context
- http://192.168.234.128
 - https://sync-702-us-west-2.sync.services.mozilla.com
 - https://safebrowsing.googleapis.com
 - http://192.168.234.128
 - GET:backup
 - GET:backup(D)
 - GET:backup(M)
 - GET:backup(N)
 - GET:backup(S)

Header: Text Body: Text

History Search 경고 Output WebSockets Spider Active Scan +

New Scan 진행: 0: http://192.168.234.128 31% 현재 검색: 1 Num requests: 3636 Export

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
5,557	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/images	200	OK	35 ms	270 bytes	242 bytes
5,558	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/icons	404	Not Found	37 ms	168 bytes	271 bytes
5,559	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/icons/blank.gif	200	OK	2 ms	255 bytes	216 bytes
5,560	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/icons/text.gif	404	Not Found	1 ms	168 bytes	280 bytes
5,561	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/icons/image2.gif	200	OK	2 ms	256 bytes	309 bytes
5,562	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/icons/unknown.gif	404	Not Found	2 ms	168 bytes	283 bytes
5,564	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/images	301	Moved Permane...	35 ms	274 bytes	306 bytes
5,565	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/images/	200	OK	35 ms	141 bytes	3,572 bytes
5,566	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/images/1000.jpg	200	OK	3 ms	258 bytes	2,804 bytes
5,568	18. 12. 19 오후 11:21:41	18. 12. 19 오후 11:21:41	GET	http://192.168.234.128/images	301	Moved Permane...	34 ms	274 bytes	306 bytes

Alerts 1 2 5 0 Current Scans 0 0 1 0 0 0 0 0

4. 자동 진단 도구 실습

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu bar includes File, Edit, View, Analyse, Report, Tools, Online, and Help. The toolbar shows various icons for file operations, analysis, and reporting. The main window is divided into several panes:

- Left Pane:** Shows a tree view of sites and requests. The selected site is `http://192.168.234.128`. The selected request is `GET:backup`.
- Header/Body Pane:** Displays the HTTP response details. The status is `HTTP/1.1 200 OK`. The body contains HTML code, including a table with a row containing a link to `/cgi-bin/badstore.cgi?action=cartview` and a script tag: `<script>alert(1);</script>`.
- Bottom Pane:** Shows the results of the scan. The selected issue is `Cross Site Scripting (Reflected)`. The details include:
 - URL: `http://192.168.234.128/cgi-bin/badstore.cgi?action=moduser`
 - 위험: High
 - Confidence: Medium
 - 매개 변수: fullname
 - 공격: `<script>alert(1);</script>`
 - Evidence: `<script>alert(1);</script>`
 - CWE ID: 79
 - WASC ID: 8
 - Source: Active (40012 - Cross Site Scripting (Reflected))

The bottom status bar shows the number of alerts (3), errors (3), warnings (5), and other issues (0). The current scans section shows 0 scans in progress.

Summary of Alerts

Alert Detail

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://192.168.234.128/cgi-bin/badstore.cgi?action=cartadd
Method	POST
Parameter	cartitem
Attack	1005' AND '1'='1' --
URL	http://192.168.234.128/cgi-bin/badstore.cgi?action=supplierportal
Method	POST
Parameter	email
Attack	ZAP' OR '1'='1' --
URL	http://192.168.234.128/cgi-bin/badstore.cgi?action=search&action=supupload&searchquery=ZAP%27+AND+%271%27%3D%271%27+--+
Method	GET
Parameter	searchquery

취약점 진단

4. 수동 보조 진단 도구 실습

Burp Suite Community Edition v1.7.36 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Site map Scope

Logging of out-of-scope Proxy traffic is disabled [Re-enable]

Filter: Hiding out of scope and 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
http://192.168.234.128	GET	/cgi-bin/badstore.cgi		200	4289	HTML	Welcome to BadStore.ne...		12:02:02 21 ...
http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	4351	HTML	Welcome to BadStore.ne...		12:03:50 21 ...
http://192.168.234.128	GET	/cgi-bin/badstore.cgi?acti...	✓	200	5043	HTML	BadStore.net - View Car...		12:03:53 21 ...
http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	12467	HTML	Welcome to the BadStor...		12:04:33 21 ...
http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	12467	HTML	Welcome to the BadStor...		12:23:45 21 ...
http://192.168.234.128	GET	/cgi-bin/badstore.cgi?acti...	✓	200	4674	HTML	BadStore.net - Sign our ...		12:04:21 21 ...
http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	4201	HTML	BadStore.net - Login Error		12:03:09 21 ...

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Date: Thu, 20 Dec 2018 03:53:39 GMT
Server: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
Cache-Control: no-cache
ETag: CPE1704TKS
Pragma: no-cache
Connection: close
Content-Type: text/html
Content-Length: 4046

<BODY bgColor=#ffffff leftMargin=0 topMargin=0 MARGINHEIGHT="0" MARGINWIDTH="0">

<TABLE cellSpacing=0 cellPadding=0 width=760 bgColor=#004b2c border=0>

<TBODY>

<TR>

<TD width=326 bgColor=#004b2c>

</TD></TR></TBODY></TABLE>

<TABLE cellSpacing=0 cellPadding=0 width=760 border=0>

<TBODY>

<TR valign=top align=left>

<TD valign=top width=143 bgColor=#e0e0e0>

<TABLE cellSpacing=0 cellPadding=0 width=143 bgColor=#004b2c border=0>

<FORM name=search onSubmit=/cgi-bin/badstore.cgi method=get>

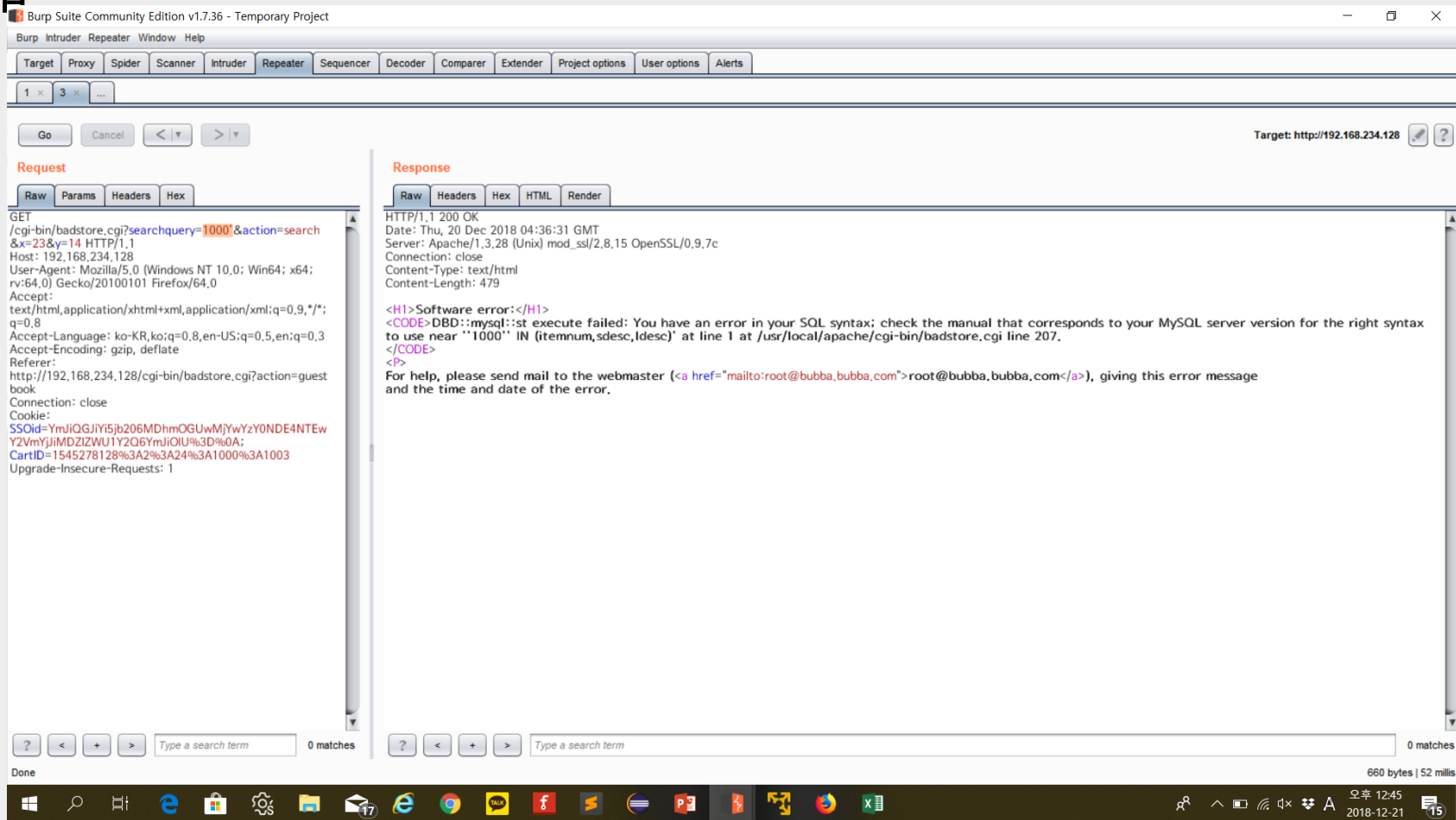
<TBODY>

<TR>

0 matches

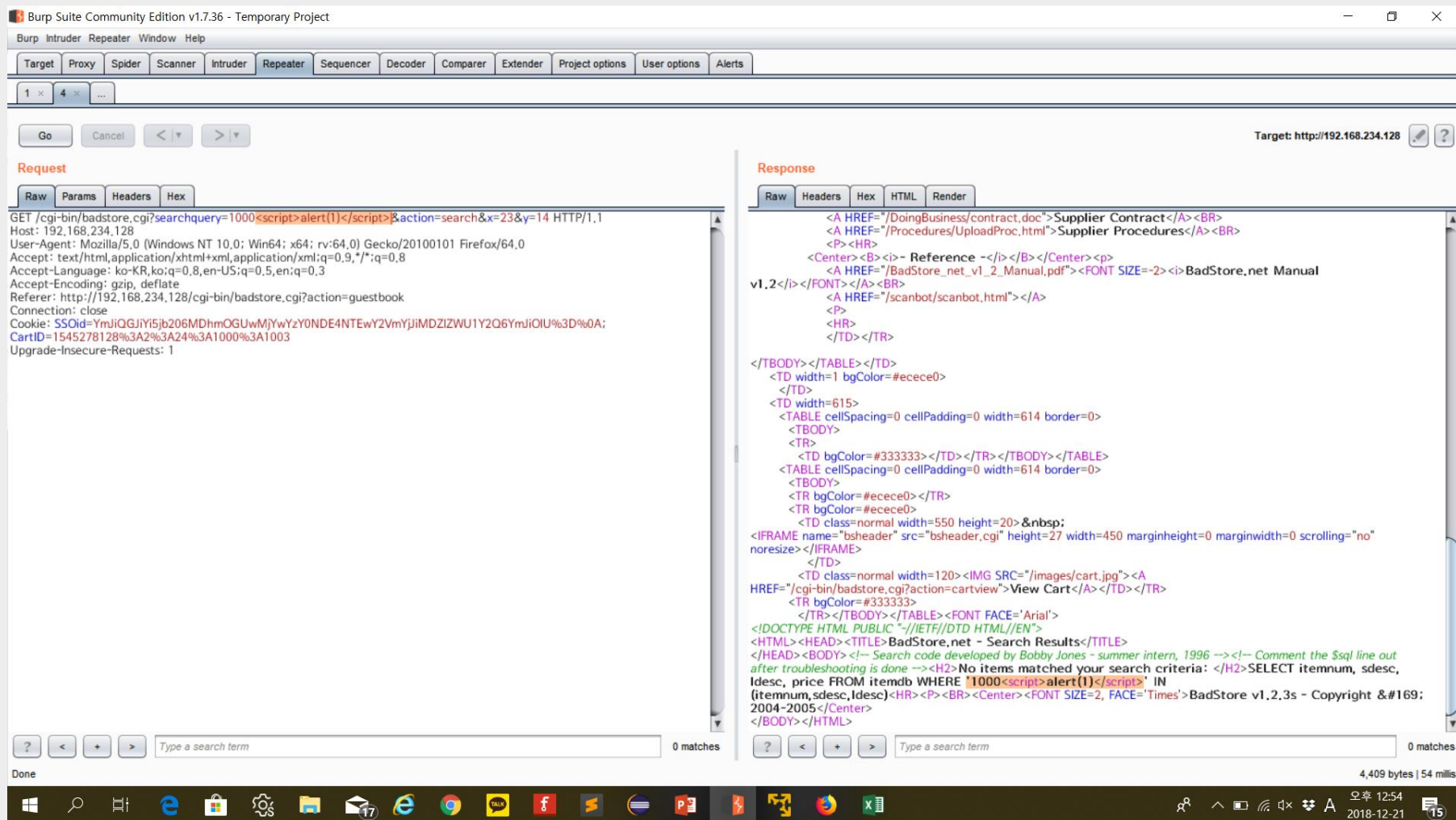
취약점 진단

4. 자동 보조 진단 도구 실습



취약점 진단

4. 수동 보조 진단 도구



감사합니
다.

Session Properties

▼ Session

General

Exclude from Proxy

Exclude from Scanner

Exclude from Spider

▼ Contexts

▶ 1:Default Context

▼ 2:http://192.168.234.128

2: Include in Context

2: Exclude from Context

2: Structure

2: Technology

2: Authentication

2: Users

2: Forced User

2: Session Management

2: Authorization

2: Alert Filters

Exclude from WebSockets

2: Authentication

Currently selected Authentication method for the Context:

Form-based Authentication

Configure Authentication Method

Login Form Target URL *:

2.168.234.128/cgi-bin/badstore.cgi?action=register

Select...

Login Request POST Data (if any):

aaa.com&passwd=aaa&pwdhint=green&role=U&Register=Register

Username Parameter *:

email

Password Parameter *:

passwd

The *username* and *password* fields will be replaced, during authentication, with the username and password corresponding to application's users.

Regex pattern identified in Logged In response messages:

Regex pattern identified in Logged Out response messages:

취소

확인

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
▶ http://192.168.234.128	http://192.168.234.128	GET	/cardvrfy.js		200	1461	script			12:03:56 21 ...
▶ https://api.accounts.firefox.com	http://192.168.234.128	GET	/cgi-bin/badstore.cgi		200	4289	HTML	Welcome to BadStore.ne...		12:02:02 21 ...
▶ https://aus5.mozilla.org	http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	4351	HTML	Welcome to BadStore.ne...		12:03:50 21 ...
▶ https://bugzilla.mozilla.org	http://192.168.234.128	GET	/cgi-bin/badstore.cgi?acti...	✓	200	5043	HTML	BadStore.net - View Car...		12:03:53 21 ...
▶ https://ciscobinary.openh264.org	http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	12467	HTML	Welcome to the BadStor...		12:04:33 21 ...
▶ http://detectportal.firefox.com	http://192.168.234.128	GET	/cgi-bin/badstore.cgi?acti...	✓	200	4674	HTML	BadStore.net - Sign our ...		12:04:21 21 ...
▶ https://docs.google.com	http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	4201	HTML	BadStore.net - Login Error		12:02:59 21 ...
▶ https://firefox.settings.services.mozilla.com	http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	4201	HTML	BadStore.net - Login Error		12:03:09 21 ...
▶ https://ftp.mozilla.org	http://192.168.234.128	GET	/cgi-bin/badstore.cgi?acti...	✓	200	5480	HTML	BadStore.net - Register/...		12:02:00 21 ...
▶ https://getpocket.cdn.mozilla.net	http://192.168.234.128	POST	/cgi-bin/badstore.cgi?acti...	✓	200	4390	HTML	Welcome to BadStore.ne...		12:03:23 21 ...
▶ https://getpocket.com										
▶ https://github.com										
▶ https://incoming.telemetry.mozilla.org										
▶ http://json-schema.org										
▶ https://net-mozaws-prod-us-west-2-normandy.s3.amaz										
▶ https://normandy.cdn.mozilla.net										
▶ https://normandy.services.mozilla.com										
▶ https://profile.accounts.firefox.com										
▶ https://push.services.mozilla.com										
▶ https://qsurvey.mozilla.com										
▶ https://r4---sn-ab02a0nfpqxapox-bh2ez.gvt1.com										
▶ https://redirector.gvt1.com										
▶ https://search.services.mozilla.com										
▶ https://services.addons.mozilla.org										
▶ https://shavar.services.mozilla.com										
▶ https://snippets.cdn.mozilla.net										
▶ https://support.mozilla.org										
▶ https://sync-702-us-west-2.sync.services.mozilla.com										
▶ https://tiles.services.mozilla.com										
▶ https://token.services.mozilla.com										
▶ https://versioncheck-bg.addons.mozilla.org										
▶ https://wiki.mozilla.org										
▶ https://www.google.com										
▶ https://www.mozilla.org										

Request Response

Raw Headers Hex

GET /cgi-bin/badstore.cgi HTTP/1.1
Host: 192.168.234.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.234.128/cgi-bin/badstore.cgi?action=loginregister
Connection: close
Upgrade-Insecure-Requests: 1

? < + > Type a search term

0 matches

BS BadStore.net - Search Results

BadStore.net - Search Results

←

→

×

🏠

192.168.234.128/cgi-bin/badstore.cgi?se

...

🔒

☆

↓

📁

📄

☰

BADSTORE.NET

Quick Item Search



Welcome **bbb** - Cart contains 2 items at \$24.00

 [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](#)

No items matched your search criteria:

SELECT itemnum, sdesc, ldesc, price FROM itemdb WHERE '1000'

1

확인

192.168.234.128 전송 중...