

〈부분 암호화 소스 설정 방법〉

보안서버를 정상적으로 구동시키기 위해서는 보안서버를 서버에 설치하는 것 이외에도 웹페이지에 적용하는 작업이 필요합니다. 보안서버를 웹페이지에 적용하는 방법으로는 전체 페이지를 암호화 하는 방법과 부분페이지를 암호화 하는 방법이 있습니다.

전체 페이지를 암호화 하는 방법은 아주 간단한 소스 수정을 통하여 적용할 수 있으나 암호화 적용이 필요 없는 부분까지 암호화하기 때문에 부분 암호화 보다는 서버에 부하를 줄 수 있습니다. 부분 페이지 암호화는 전체 페이지를 암호화 하는 것 보다 소스 수정 부분이 조금 더 복잡하지만 서버의 부하가 증가하는 것을 줄일 수 있습니다.

부분 암호화는 다시 페이지별 암호화와 프레임 암호화로 나누어 설명을 드리도록 하겠습니다.

가. 페이지별 암호화

페이지별 암호화는 현재 위치하고 있는 페이지에서 다른 페이지로 이동할 때, 보안을 위해서 암호화된 전송을 할 것인지 아니면 평문 전송할 것인지를 선택하여 암호화하는 것을 말합니다. 부분적인 페이지 암호화를 사용하는 이유는 위에서 언급한 바와 같이 암호화 적용이 필요 없는 부분까지 암호화를 하여 서버의 부하를 증가시키는 것을 최대한 줄일 수 있기 때문입니다.

다음 <그림 1>은 웹 페이지의 메뉴 부분 예입니다. 이 중 ‘서버관련 강좌 & TIP’ 메뉴를 클릭하여 이동을 하면 https가 호출되어 서버와 클라이언트간의 통신이 암호화되어 전송되고, ‘Q&A’ 메뉴를 클릭하여 이동하면 http가 호출되어 서버와 클라이언트간의 통신이 평문으로 이루어지

게 하는 방법을 알아보겠습니다.



<그림 1> 페이지별 암호화 대상 메뉴

<그림 2>은 위 메뉴 부분의 소스코드입니다. 밑줄 부분 중 첫 번째 밑줄에 해당하는 부분이 현재 위치에서 메뉴를 클릭하여 이동할 때 암호화 전송을 하도록 하게끔 설정된 것이고, 두 번째 밑줄은 현재 위치에서 메뉴를 클릭하여 이동할 때 평문 전송을 하도록 설정된 것입니다.

```
<map name="ImageMap1">
<area shape="rect" coords="193, 74, 249, 90" href="onlinebook/online.htm" target="main">
<area shape="rect" coords="267, 75, 401, 89" href="https://[redacted].co.kr/zboard/zboard.php?id=lecture" target="_top">
<area shape="rect" coords="423, 73, 479, 89" href="https://[redacted].co.kr/zboard/zboard.php?id=problem" target="_top">
<area shape="rect" coords="497, 73, 537, 89" href="http://[redacted].co.kr/zboard/zboard.php?id=qna" target="_top">
<area shape="rect" coords="555, 73, 609, 89" href="http://[redacted].co.kr/zboard/zboard.php?id=down" target="_top">
<area shape="rect" coords="679, 5, 717, 23" href="index.html" target="_top">
```

<그림 2> 페이지별 암호화 대상 메뉴의 소스코드

위 그림을 참조하시어 웹 페이지의 소스를 수정하시고 부분 암호화를 적용하시기 바랍니다.

나. 프레임 암호화

부분 페이지별 암호화 이외에도 프레임별로 암호화 하는 방식도 존재하고 있습니다. 프레임이 삽입된 웹페이지의 경우에는 암호화된 페이지와 비 암호화된 페이지를 각각 적용시킬 수 있습니다.

<그림 3>과 같이 웹페이지(index.html)에 프레임으로 두 개의 페이지 topmenu.htm과 main.htm을 불러오는 원본 소스코드가 있습니다.

```

<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=euc-kr">
<title>SSL Frame Test</title>
</head>
<frameset rows="100, 1*" border="1">
  <frame src="http://lab.████████.co.kr/test_ssl/topmenu.htm" scrolling="yes" name="top" namo_target_frame="main">
  <frame src="http://lab.████████.co.kr/test_ssl/main.htm" scrolling="yes" name="main">
  <noframes>
  <body bgcolor="white" text="black" link="blue" vlink="purple" align="red">
  <p>SSL Frame Test의 페이지 입니다. <br> 이페이지를 보기 위해서는 프레임을 볼수 있는 웹 브라우저가 필요합니다.</p>
  </body>
  </noframes>
</frameset>
</html>

```

<그림 3> 프레임이 포함된 웹페이지

이때 topmenu.htm 소스코드만 URL을 <그림 4>처럼 https로 변경합니다.

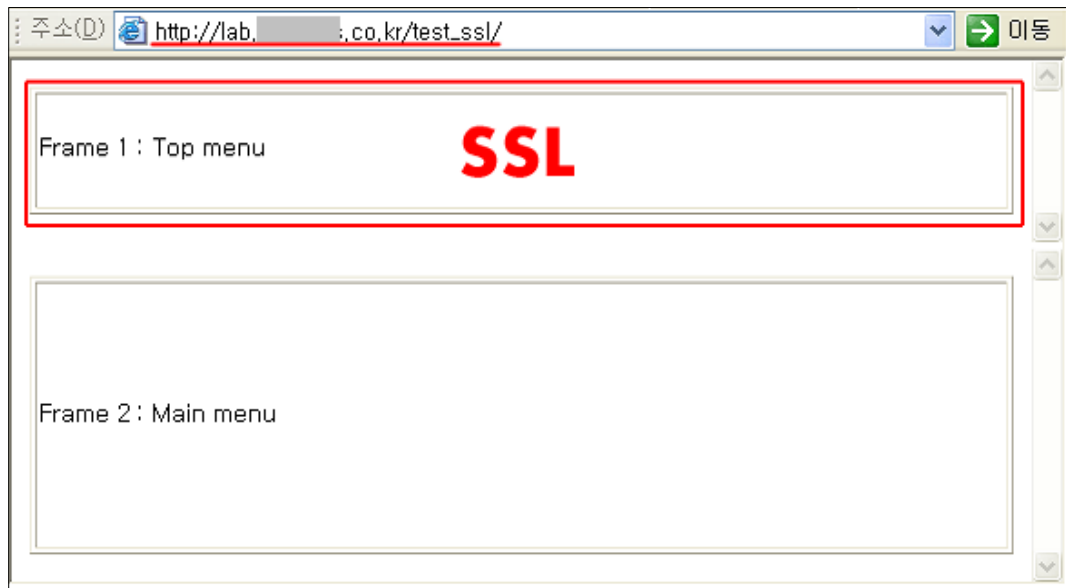
```

<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=euc-kr">
<title>SSL Frame Test</title>
</head>
<frameset rows="100, 1*" border="1">
  <frame src="https://lab.████████.co.kr/test_ssl/topmenu.htm" scrolling="yes" name="top" namo_target_frame="main">
  <frame src="http://lab.████████.co.kr/test_ssl/main.htm" scrolling="yes" name="main">
  <noframes>
  <body bgcolor="white" text="black" link="blue" vlink="purple" align="red">
  <p>SSL Frame Test의 페이지 입니다. <br> 이페이지를 보기 위해서는 프레임을 볼수 있는 웹 브라우저가 필요합니다.</p>
  </body>
  </noframes>
</frameset>
</html>

```

<그림 4> topmenu.htm을 https로 호출하기

적용을 완료하고 <그림 5>와 같이 웹 브라우저를 http로 호출하여도 <그림 6>처럼 암호화가 이루어지는 것을 확인 할 수 있습니다.



<그림 5> topmenu.htm만 암호화하여 호출하기

```

T 211. .... :80 -> 211. .... :4188 [AP]
HTTP/1.1 200 OK..Date: Mon, 26 Feb 2007 07:24:28 GMT..Server: Ap
ache..X-Powered-By: PHP/4.3.8..Keep-Alive: timeout=15, max=100..
Connection: Keep-Alive..Transfer-Encoding: chunked..Content-Type
: text/html....27d..<html>..<head>..<meta http-equiv="content-typ
e" content="text/html; charset=euc-kr">..<title>SSL Frame Test</t
itle>..</head>..<frameset rows="100, 1*" border="1">.. <frame src
="https://lab.firewalls.co.kr/test_ssl/topmenu.htm" scrolling="y
es" name="top" namo_target_frame="main">.. <frame src="http://
lab.firewalls.co.kr/test_ssl/main.htm" scrolling="yes" name="mai
n">.. <noframes>.. <body bgcolor="white" text="black" link="
blue" vlink="purple" alink="red">.. <p>SSL Frame Test.. ..
..... <br> ..
..... </p>.. </body>.. </noframes>..</fra
meset>..</html>....0....
#
T 211. .... :4188 -> 211. .... :80 [AP]
GET /test_ssl/main.htm HTTP/1.1..Accept: image/gif, image/x-ubit
map, image/jpeg, image/pjpeg, application/x-shockwave-flash, app
lication/vnd.ms-excel, application/vnd.ms-powerpoint, applicatio
n/msword, */*..Referer: http://lab.firewalls.co.kr/test_ssl/..Ac
cept-Language: ko..Accept-Encoding: gzip, deflate..User-Agent: M
ozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4
322)..Host: lab.firewalls.co.kr..Connection: Keep-Alive....
#
T 211. .... :80 -> 211. .... :4188 [AP]
HTTP/1.1 200 OK..Date: Mon, 26 Feb 2007 07:24:28 GMT..Server: Ap
ache..X-Powered-By: PHP/4.3.8..Keep-Alive: timeout=15, max=99..C
onnection: Keep-Alive..Transfer-Encoding: chunked..Content-Type:
text/html....77 ...<html>..<body>..<table width=100% height=100%
border=1>..<tr><td>.Frame 2 : Main menu.</td></tr>..</table>..</bod
y>..</html>..0....
#exit

```

<그림 6> topmenu.htm의 내용만 암호화된 모니터링 결과

단, 프레임별로 암호화를 제공하는 경우 암호화가 제공되는 부분과 암호화가 제공되지 않는 부분이 공존하도록 구성이 가능하여 소스 수정에 착오가 생길 수 있습니다.

예를 들어 아무리 프레임이 https 설정이 되어있다면 http로 호출하여도

암호화가 이루어지지만, 반대로 https를 이용해서 호출을 했어도 프레임이 https 주소를 가지고 있지 않다면 암호화가 되지 않고 정보의 노출이 발생할 수 있습니다. 그러므로 프레임이 사용되는 페이지에서 부분 암호화를 적용하였을 경우 https로 호출하여 암호화 여부를 꼭 확인을 하여야 합니다.