SECURE CODING

TEAM 12 - PHASE 4

MEMBERS

Alexander Lill
Lorenzo Donini
Florian Mauracher
Mahmoud Naser

FIX ALL THE BUGS


ONE DOES NOT SIMPLY
FIX ALL THE BUGS

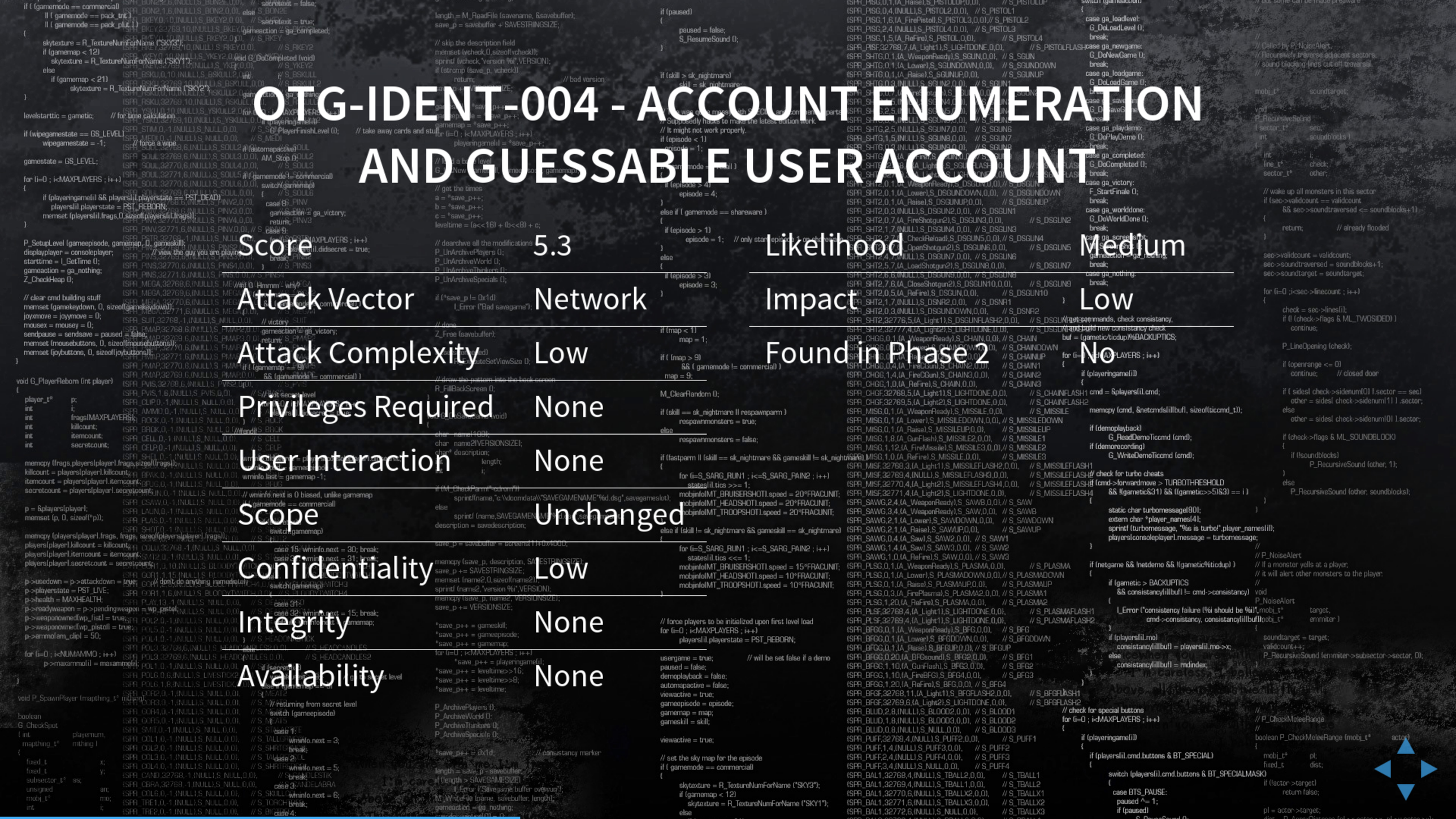

TEAM 7
TOP VULNERABILITIES

OTG-CONFIG-003 - FILE EXTENSIONS HANDLING FOR SENSITIVE INFORMATION

Score	5.9	Likelihood	Medium
Attack Vector	Network	Impact	High
Attack Complexity	High	Found in Phase 2	Yes
Privileges Required	None		
User Interaction	None		
Scope	Unchanged		
Confidentiality	High		
Integrity	None		
Availability	None		

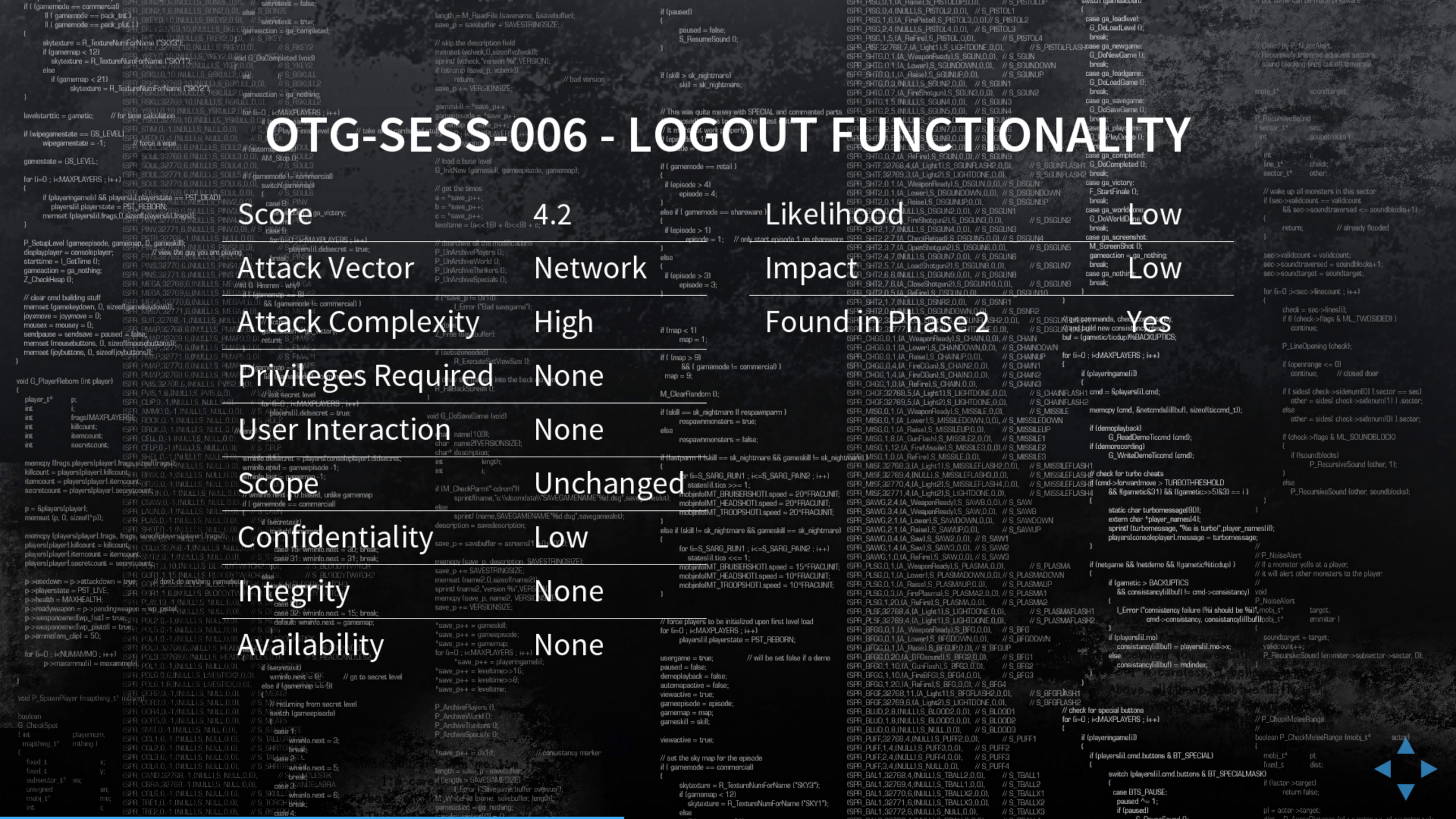
OTG-IDENT-004 - ACCOUNT ENUMERATION AND GUESSABLE USER ACCOUNT

Score	5.3	Likelihood	Medium
Attack Vector	Network	Impact	Low
Attack Complexity	Low	Found in Phase 2	No
Privileges Required	None		
User Interaction	None		
Scope	Unchanged		
Confidentiality	Low		
Integrity	None		
Availability	None		



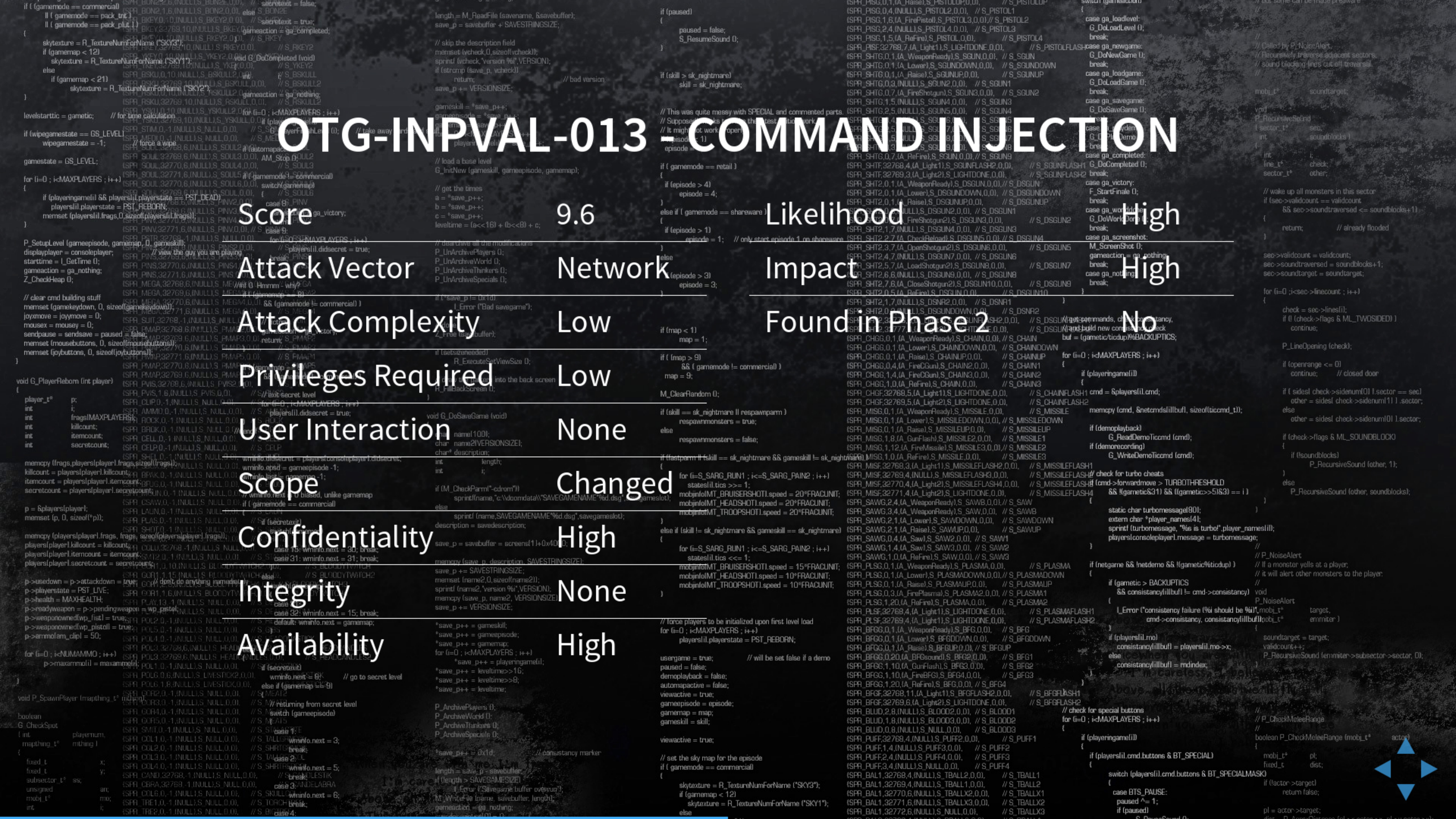
OTG-SESS-006 - LOGOUT FUNCTIONALITY

Score	4.2	Likelihood	Low
Attack Vector	Network	Impact	Low
Attack Complexity	High	Found in Phase 2	Yes
Privileges Required	None		
User Interaction	None		
Scope	Unchanged		
Confidentiality	Low		
Integrity	None		
Availability	None		



OTG-INPVAL-013 - COMMAND INJECTION

Score	9.6	Likelihood	High
Attack Vector	Network	Impact	High
Attack Complexity	Low	Found in Phase 2	No
Privileges Required	Low		
User Interaction	None		
Scope	Changed		
Confidentiality	High		
Integrity	None		
Availability	High		



OTG-INPVAL-014-3 - HEAP OVERFLOW

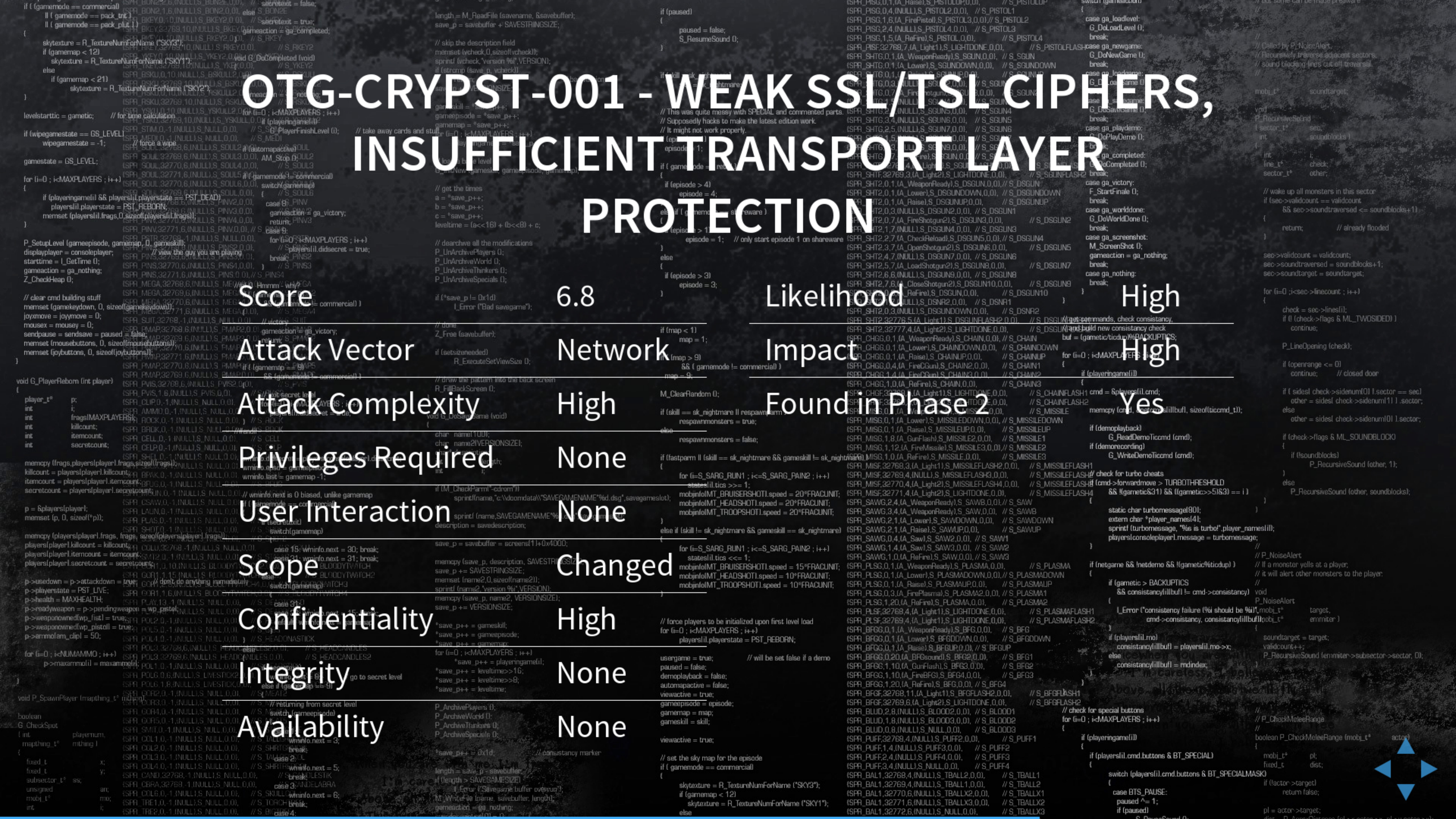
Score	3.3	Likelihood	Low
Attack Vector	Local	Impact	Low
Attack Complexity	Low	Found in Phase 2	No
Privileges Required	Low		
User Interaction	None		
Scope	Unchanged		
Confidentiality	None		
Integrity	Low		
Availability	None		

OTG-ERR-002 - ANALYSIS OF STACK TRACES

Score	5.3	Likelihood	High
Attack Vector	Network	Impact	Low
Attack Complexity	Low	Found in Phase 2	Yes
Privileges Required	None		
User Interaction	None		
Scope	Unchanged		
Confidentiality	Low		
Integrity	None		
Availability	None		

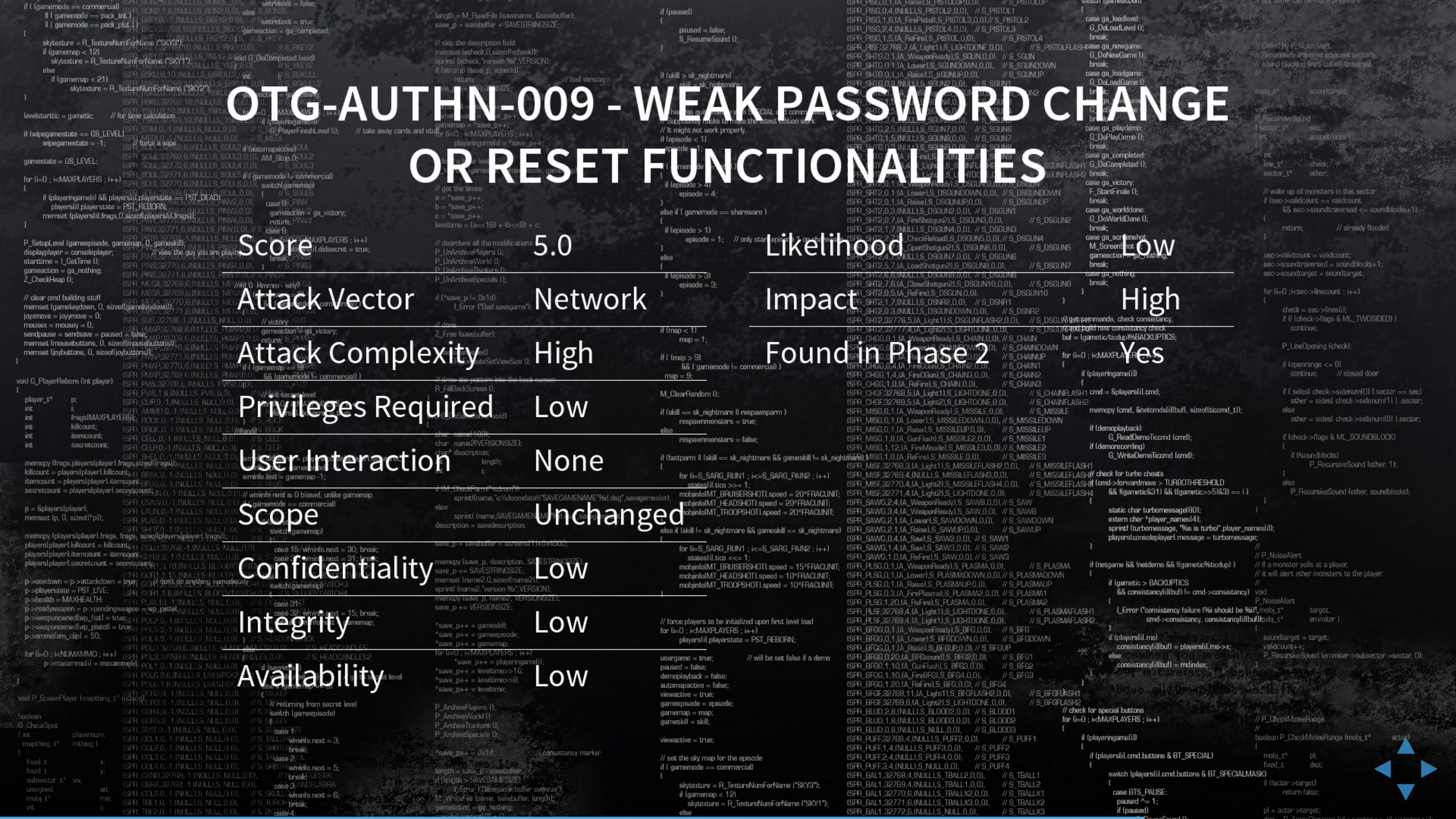
OTG-CRYPST-001 - WEAK SSL/TSL CIPHERS, INSUFFICIENT TRANSPORT LAYER PROTECTION

Score	6.8	Likelihood	High
Attack Vector	Network	Impact	High
Attack Complexity	High	Found in Phase 2	Yes
Privileges Required	None		
User Interaction	None		
Scope	Changed		
Confidentiality	High		
Integrity	None		
Availability	None		



OTG-AUTHN-009 - WEAK PASSWORD CHANGE OR RESET FUNCTIONALITIES

Score	5.0	Likelihood	Low
Attack Vector	Network	Impact	High
Attack Complexity	High	Found in Phase 2	Yes
Privileges Required	Low		
User Interaction	None		
Scope	Unchanged		
Confidentiality	Low		
Integrity	Low		
Availability	Low		



OTG-SESS-005 - CROSS SITE REQUEST FORGERY

Score	4.2	Likelihood	Medium
Attack Vector	Network	Impact	Medium
Attack Complexity	High	Found in Phase 2	Yes
Privileges Required	None		
User Interaction	Required		
Scope	Unchanged		
Confidentiality	Low		
Integrity	Low		
Availability	None		

DEMO

THANKS FOR YOUR ATTENTION!